Release Notes for the Catalyst 3750, 3560, and 2970 Switches, Cisco IOS Release 12.2(20)SE3

Revised April 2005

The Cisco IOS Release 12.2(20)SE3 runs on Catalyst 3750, 3560, and 2970 switches.

The Catalyst 3750 switches support stacking through Cisco StackWise technology. The Catalyst 3560 and 2970 switches do not support switch stacking. Unless otherwise noted, the term *switch* refers to a standalone switch and to a switch stack.

These release notes include important information about this Cisco IOS release and any limitations, restrictions, and caveats that apply to it. Verify that these release notes are correct for your switch:

- If you are installing a new switch, refer to the Cisco IOS release label on the rear panel of your switch.
- If your switch is on, use the **show version** privileged EXEC command. See the "Finding the Software Version and Feature Set" section on page 5.
- If you are upgrading to a new release, refer to the software upgrade filename for the software version. See the "Deciding Which Files to Use" section on page 6.

For the complete list of Catalyst 3750, 3560, and 2970 switch documentation, see the "Related Documentation" section on page 65.

You can download the switch software from these sites:

- http://www.cisco.com/kobayashi/sw-center/sw-lan.shtml

  (for registered Cisco.com users with a login password)
- http://www.cisco.com/public/sw-center/sw-lan.shtml

  (for nonregistered Cisco.com users)

This software release is part of a special release of Cisco IOS software that is not released on the same 8-week maintenance cycle that is used for other platforms. As maintenance releases and future software releases become available, they will be posted to Cisco.com (previously Cisco Connection Online [CCO]) in the Cisco IOS software area.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

This information is in the release notes:

- "System Requirements" section on page 2
- "Downloading Software" section on page 5
- "Installation Notes" section on page 8
- "New Features" section on page 8
- "New Software Features" section on page 9
- "Limitations and Restrictions" section on page 10
- "Important Notes" section on page 21
- "Open Caveats" section on page 22
- "Resolved Caveats" section on page 28
- "Documentation Updates" section on page 34
- "Related Documentation" section on page 65
- "Obtaining Documentation" section on page 66
- "Documentation Feedback" section on page 66
- "Obtaining Technical Assistance" section on page 67
- "Obtaining Additional Publications and Information" section on page 68

System Requirements

The system requirements are described in these sections:

- "Hardware Supported" section on page 2
- "Software Compatibility" section on page 4
- "Cluster Compatibility" section on page 4

Hardware Supported

Table 1 lists the hardware supported on Cisco IOS Release 12.2SE.

Table 1 Catalyst 3750, 3560, and 2970 Supported Hardware

Switch	Description	Supported by Minimum Cisco IOS Release
Catalyst 3750G-12S	12 SFP[1] module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3750-24TS	24 10/100 Ethernet ports and 2 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3750G-24T	24 10/100/1000 Ethernet ports	Cisco IOS Release 12.2(18)SE
Catalyst 3750G-24TS	24 10/100/1000 Ethernet ports and 4 SFP module slots	Cisco IOS Release 12.2(18)SE

Table 1 Catalyst 3750, 3560, and 2970 Supported Hardware (continued)

Switch	Description	Supported by Minimum Cisco IOS Release
Catalyst 3750-48TS	48 10/100 Ethernet ports and 4 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3750G-48TS	48 10/100/1000 Ethernet ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3750G-24TS-1U	24 10/100/1000 Ethernet ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3750-24PS	24 10/100 PoE[2] ports and 2 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3750G-24PS	24 10/100/1000 PoE ports and 4SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3750-48PS	48 10/100 PoE ports and 4 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3750G-48PS	48 10/100/1000 PoE ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3750G-16TD	16 10/100/1000 ports and 1 XENPAK 10-Gigabit Ethernet module port	Cisco IOS Release 12.2(18)SE1
Catalyst 3560-24PS	24 10/100 PoE ports and 2 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3560-48PS	48 10/100 PoE ports and 4 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3560G-24PS	24 10/100/1000 PoE ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3560G-48PS	48 10/100/1000 PoE ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3560G-24TS	24 10/100/1000 ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3560G-48TS	48 10/100/1000 ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 2970G-24T	24 10/100/1000 Ethernet ports	Cisco IOS Release 12.2(18)SE
Catalyst 2970G-24TS	24 10/100/1000 Ethernet ports and 4 SFP module slots	Cisco IOS Release 12.2(18)SE
SFP modules	1000BASE-T, 1000BASE-SX, 1000BASE-LX, 1000BASE-ZX, and CWDM[3] 100BASE-FX MMF[4]	Cisco IOS Release 12.2(18)SE Cisco IOS Release 12.2(20)SE1
Redundant power systems	Cisco RPS 675 Redundant Power System	Supported on all software releases

1. SFP = small form-factor pluggable
2. PoE = Power over Ethernet
3. CWDM = coarse wavelength-division multiplexer
4. MMF = multimode fiber

Software Compatibility

For hardware requirements, operating system, and browser recommendations for running the Cluster Management Suite (CMS), refer to the "Getting Started with CMS" chapter in the software configuration guide.

Windows

This release uses a CMS plug-in to run CMS. You can download the latest CMS plug-in for Windows from this URL:

http://www.cisco.com/pcgi-bin/Support/ClusterMgmtSuite/cms_plugin_redirect.cgi?platform=windows&version=1.1

Solaris

This release uses a CMS plug-in that replaces the Java plug-in. You can download the latest CMS plug-in for Solaris from this URL:

http://www.cisco.com/pcgi-bin/Support/ClusterMgmtSuite/cms_plugin_redirect.cgi?platform=solaris&version=1.1

Cluster Compatibility

This section describes how to choose command and standby command switches when a cluster consists of a mixture of Catalyst switches. When creating a switch cluster or adding a switch to a cluster, follow these guidelines:

- When you create a switch cluster, Cisco recommends configuring the highest-end switch in your cluster as the command switch. Table 2 lists the cluster capabilities and Cisco IOS releases for the switches. The switches are listed from the highest to lowest end.
- If you are managing the cluster through CMS, the switch that has the latest software should be the command switch, *unless* your command switch is running Cisco IOS Release 12.1(19)EA1 or later.
- The standby command switch must be the same type as the command switch. For example, if the command switch is a Catalyst 3750 switch, all standby command switches must be Catalyst 3750 switches.

Table 2 Switch Software and Cluster Capability

Switch	Cisco IOS Release	Cluster Capability
Catalyst 3750	12.1(11)AX or later	Member or command switch
Catalyst 3560	12.1(19)EA1b or later	Member or command switch
Catalyst 3550	12.1(4)EA1 or later	Member or command switch
Catalyst 2970	12.1(11)AX or later	Member or command switch
Catalyst 2955	12.1(12c)EA1 or later	Member or command switch
Catalyst 2950	12.0(5.2)WC(1) or later	Member or command switch
Catalyst 2950 LRE	12.1(11)JY or later	Member or command switch
Catalyst 2940	12.1(13)AY or later	Member or command switch

Table 2 Switch Software and Cluster Capability (continued)

Switch	Cisco IOS Release	Cluster Capability
Catalyst 3500 XL	12.0(5.1)XU or later	Member or command switch
Catalyst 2900 XL (8-MB switches)	12.0(5.1)XU or later	Member or command switch
Catalyst 2900 XL (4-MB switches)	11.2(8.5)SA6 (recommended)	Member switch only[1]
Catalyst 1900 and 2820	9.00(-A or -EN) or later	Member switch only

1. Catalyst 2900 XL (4-MB) switches appear in the front-panel and topology views of the CMS. However, CMS does not support the configuration or the monitoring of these switches.

CMS is not forward-compatible on command switches running Cisco Release IOS 12.1(14)EA1 and earlier. This means that if a member switch is running a release that is earlier than the release running on the command switch, the new features are not available on the member switch. If the member switch is a new device running a release that is later than the release on the command switch, the command switch cannot recognize the member switch, and the Front Panel view displays it as an unknown device. You cannot configure any parameters or generate a report through CMS for that member; instead, you must launch the Device Manager application to configure and to obtain reports for that member.

If you have a cluster with switches that are running different versions of Cisco IOS software, features added on the latest release might not be reflected on switches running the older releases. For example, if you start CMS on a Catalyst 2900 XL switch running Cisco IOS Release 11.2(8)SA6, the windows and functionality can be different from a switch running Cisco IOS Release 12.0(5)WC(1) or later.

Some early Cisco IOS releases do not support clustering.

For more information about clustering and CMS, refer to the software configuration guide.

Downloading Software

These are the procedures for downloading software. Before downloading software, read this section for important information:

- "Finding the Software Version and Feature Set" section on page 5
- "Deciding Which Files to Use" section on page 6
- "Upgrading a Switch by Using CMS" section on page 6
- "Upgrading a Switch by Using the CLI" section on page 7
- "Recovering from a Software Failure" section on page 8

Finding the Software Version and Feature Set

The Cisco IOS image is stored as a .bin file in a directory that is named with the Cisco IOS release. A subdirectory contains the files needed for web management. The image is stored on the system board flash device (flash:).

You can use the **show version** privileged EXEC command to see the software version that is running on your switch. The second line of the display shows the version.

Note For Catalyst 3750 and 3560 switches, although the **show version** output always shows the software image running on the switch, the model name shown at the end of this display is the factory configuration (standard multilayer image [SMI] or enhanced multilayer image [EMI]) and does not change if you upgrade the software image.

You also can use the **dir** *filesystem***:** privileged EXEC command to see the directory names of other software images that you might have stored in flash memory.

Deciding Which Files to Use

The upgrade procedures in these release notes describe how to perform the upgrade by using a combined tar file. This file contains both the Cisco IOS image file and the files needed for CMS. You must use the combined tar file to upgrade the switch through CMS. To upgrade the switch through the command-line interface (CLI), use the tar file and the **archive download-sw** privileged EXEC command.

Table 3 lists the filenames for this software release.

Table 3 Cisco IOS Software Image Files

Filename	Description
c3750-i9-tar.122-20.SE3.tar	Catalyst 3750 SMI file and CMS files
c3750-i5-tar.122-20.SE3.tar	Catalyst 3750 EMI file and CMS files
c3750-i9k91-tar.122-20.SE3.tar	Catalyst 3750 SMI cryptographic file and CMS files
c3750-i5k91-tar.122-20.SE3.tar	Catalyst 3750 EMI cryptographic file and CMS files
c3560-i9-tar.122-20.SE3.tar	Catalyst 3560 SMI file and CMS files
c3560-i5-tar.122-20.SE3.tar	Catalyst 3560 EMI file and CMS files
c3560-i9k91-tar.122-20.SE3.tar	Catalyst 3560 SMI cryptographic file and CMS files
c3560-i5k91-tar.122-20.SE3.tar	Catalyst 3560 EMI cryptographic file and CMS files
c2970-i6l2-tar.122-20.SE3.tar	Catalyst 2970 image file and CMS files
c2970-i6k91l2-tar.122-20.SE3.tar	Catalyst 2970 cryptographic image file and CMS files

Upgrading a Switch by Using CMS

You can upgrade switch software by using CMS. From the feature bar, choose **Administration > Software Upgrade**. For detailed instructions, click **Help**.

Note When using HTTP to upgrade member switches, the command switch must be running *either* Cisco IOS 12.1(20)EA2 or Cisco IOS 12.2(20)SE or later. The cluster members that are upgraded must be running Cisco IOS 12.2(20)SE or later.

Upgrading a Switch by Using the CLI

This procedure is for copying the combined tar file to the switch. You copy the file to the switch from a TFTP server and extract the files. You can download an image file and replace or keep the current image.

To download software, follow these steps:

Step 1 Use Table 3 on page 6 to identify the file that you want to download.

Step 2 Download the software image file.

- If you have a SmartNet support contract, go to this URL, and log in to download the appropriate files:

  http://www.cisco.com/kobayashi/sw-center/sw-lan.shtml

- If you do not have a SmartNet contract, go to this URL, and follow the instructions to register on Cisco.com and download the appropriate files:

  http://www.cisco.com/public/sw-center/sw-lan.shtml

To download the image for a Catalyst 2970 switch, click **Catalyst 2970 software**. To obtain authorization and to download the cryptographic software files, click **Catalyst 2970 3DES Cryptographic Software**.

To download the EMI or SMI files for a Catalyst 3560 switch, click **Catalyst 3560 software**. To obtain authorization and to download the cryptographic software files, click **Catalyst 3560 3DES Cryptographic Software**.

To download the EMI or SMI files for a Catalyst 3750 switch, click **Catalyst 3750 software**. To obtain authorization and to download the cryptographic software files, click **Catalyst 3750 3DES Cryptographic Software**.

Caution If you are upgrading a Catalyst 3750 or a Catalyst 2970 switch that is running a release earlier than Cisco IOS Release 12.1(19)EA1c, this release includes a bootloader upgrade. The bootloader can take up to 1 minute to upgrade and occurs the first time that the new software is loaded. Do not power cycle the switch during the bootloader upgrade.

Step 3 Copy the image to the appropriate TFTP directory on the workstation, and make sure that the TFTP server is properly configured.

For more information, refer to Appendix B in the software configuration guide for this release.

Step 4 Log into the switch through the console port or a Telnet session.

Step 5 (Optional) Ensure that you have IP connectivity to the TFTP server by entering this privileged EXEC command:

```
ping tftp-server-address
```

For more information about assigning an IP address and default gateway to the switch, refer to the software configuration guide for this release.

Step 6 Download the image file from the TFTP server to the switch. If you are installing the same version of software that is currently on the switch, overwrite the current image by entering this privileged EXEC command:

```
archive download-sw /overwrite /reload tftp:[[//location]/directory]/image-name.tar
```

The **/overwrite** option overwrites the software image in flash memory with the downloaded one.

The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved.

For **//***location*, specify the IP address of the TFTP server.

For */directory/image-name***.tar**, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

This example shows how to download an image from a TFTP server at 198.30.20.19 and to overwrite the image on the switch:

```
Switch# archive download-sw /overwrite tftp://198.30.20.19/c3750-i5-tar.122-20.SE.tar
```

You also can download the image file from the TFTP server to the switch and keep the current image by replacing the **/overwrite** option with the **/leave-old-sw** option.

Recovering from a Software Failure

For detailed recovery procedures, refer to the "Troubleshooting" chapter in the software configuration guide for this release.

Installation Notes

You can assign IP information to your switch by using these methods:

- The Express Setup program (refer to the hardware installation guide.)
- The CLI-based setup program (refer to the hardware installation guide.)
- The DHCP-based autoconfiguration (refer to the software configuration guide.)
- Manually assigning an IP address (refer to the software configuration guide.)

Note If you are upgrading a Catalyst 3750 or a 2950 switch running Cisco IOS Release 12.1(11)AX, which uses the 802.1x feature, you must re-enable 802.1x after upgrading the software. For more information, see the "Cisco IOS Notes" section on page 21.

Note When upgrading or downgrading from Cisco IOS Release 12.2(18)SE, you might need to reconfigure the switch with the same password that you were using when running 12.2(18)SE. This problem only occurs when changing from Cisco IOS Release 12.2(18)SE to any other release. (CSCed88768)

New Features

These sections describe the supported hardware and the software features provided in this release:

- "New Hardware Features" section on page 9
- "New Software Features" section on page 9

New Hardware Features

For a list of all supported hardware, see the "Hardware Supported" section on page 2.

New Software Features

This release contains support for the temperature monitoring, fan control, and cable diagnostics features on Catalyst 3750G-24TS-1U, 3750G-48TS, 3750G-24PS, 3750G-48PS, 3560G-24TS, 3560G-24PS, 3560G-48TS, and 3560G-48PS switches.

For more information about these updates, see the "Documentation Updates for Catalyst 3750 Switches Running Cisco IOS Release 12.2(20)SE3" section on page 35 and the "Documentation Updates for Catalyst 3560 Switches Running Cisco IOS Release 12.2(20)SE3" section on page 45.

New Software Features

This release contains support for the temperature monitoring, cable diagnostics, front-end controller, and PoE features on Catalyst 3750G-24TS-1U, 3750G-48TS, 3750G-24PS, 3750G-48PS, 3560G-24TS, 3560G-24PS, 3560G-48TS, and 3560G-48PS switches..

For more information about these updates, see the "Documentation Updates for Catalyst 3750 Switches Running Cisco IOS Release 12.2(20)SE3" section on page 35.

Minimum Cisco IOS Release for Major Features

Table 4 lists the minimum software release required to support the major features of the Catalyst 3750, 3560, and 2970 switches.

Table 4 Catalyst 3750, 3560, and 2970 Switch Features and the Minimum Cisco IOS Release Required

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
802.1x accounting and MIBs (IEEE8021-PAE-MIB and CISCO-PAE-MIB)	12.2(20)SE	3750, 3560, 2970
Dynamic ARP inspection (EMI only)	12.2(20)SE	3750, 3560
Flex Links	12.2(20)SE	3750, 3560, 2970
HTTP upgrade (CMS only)	12.2(20)SE	3750, 3560, 2970
IP source guard (EMI only)	12.2(20)SE	3750, 3560
Private VLAN (EMI only)	12.2(20)SE	3750, 3560
SFP module diagnostic management interface	12.2(20)SE	3750, 3560, 2970
Switch stack offline configuration	12.2(20)SE	3750
Stack-ring activity statistics	12.2(20)SE	3750
Smartports macros	12.2(18)SE	3750, 3560, 2970

Limitations and Restrictions

You should review this section before you begin working with the switch. These are known limitations that will not be fixed, and there is not always a workaround. Some features might not work as documented, and some features could be affected by recent changes to the switch hardware or software.

These sections describe the limitations and restrictions:

- "Cisco IOS Limitations and Restrictions" section on page 10
- "Cluster Limitations and Restrictions" section on page 19
- "CMS Limitations and Restrictions" section on page 19

Cisco IOS Limitations and Restrictions

Unless otherwise noted, these limitations apply to the Catalyst 3750, 3560, and 2970 switches:

- "Configuration" section on page 10
- "Ethernet" section on page 12
- "Fallback Bridging" section on page 13
- "HSRP" section on page 13
- "IP" section on page 13
- "IP Telephony" section on page 14
- "MAC Addressing" section on page 14
- "Multicasting" section on page 14
- "QoS" section on page 15
- "Routing" section on page 15
- "SPAN and RSPAN" section on page 16
- "Stacking (Catalyst 3750 switch stack only)" section on page 17
- "Trunking" section on page 18
- "VLAN" section on page 19

Configuration

These are the configuration limitations:

- When connected to some third-party devices that send early preambles, a switch port operating at 100 Mbps full duplex or 100 Mbps half duplex might bounce the line protocol up and down. The problem is observed only when the switch is receiving frames.

  The workaround is to configure the port for 10 Mbps and half duplex or to connect a hub or a nonaffected device to the switch. (CSCed39091)

- A static IP address might be removed when the previously acquired DHCP IP address lease expires.

  This problem occurs under these conditions:

  - When the switch is booted without a configuration (no config.text file in flash memory).
  - When the switch is connected to a DHCP server that is configured to give an address to it (the dynamic IP address is assigned to VLAN 1).
  - When an IP address is configured on VLAN 1 before the dynamic address lease assigned to VLAN 1 expires.

  The workaround is to reconfigure the static IP address. (CSCea71176 and CSCdz11708)

- Certain combinations of features and switches create conflicts with the port security feature. In Table 5, *No* means that port security cannot be enabled on a port on the referenced switch if the referenced feature is also running on the same port. *Yes* means that both port security and the referenced feature can be enabled on the same port on a switch at the same time. A dash means not applicable.

Table 5 Port Security Incompatibility with Other Switch Features

	Catalyst 2940	Catalyst 2950 and Catalyst 2955	Catalyst 2970	Catalyst 3550	Catalyst 3560 and Catalyst 3750
DTP[1] port[2]	No	No	No	No	No
Trunk port	No	No	Yes	Yes	Yes
Dynamic-access port[3]	No	No	No	No	No
Routed port	—	—	—	No	No
SPAN source port	Yes	Yes	Yes	Yes	Yes
SPAN destination port	No	No	No	No	No
EtherChannel	No	No	No	No	No
Tunneling port	—	—	—	Yes	—
Protected port	Yes	Yes	Yes	Yes	Yes
802.1x port	—	Yes[4]	Yes	Yes	Yes
Voice VLAN port[5]	Yes	Yes	Yes	Yes	Yes
Private VLAN port	—	—	—	—	No[6]
IP source guard	—	—	—	—	Yes[6]
Dynamic ARP[7] inspection	—	—	—	—	Yes[6]
Flex Links	—	—	Yes	—	Yes

1. DTP = Dynamic Trunking Protocol
2. A port configured with the **switchport mode dynamic** interface configuration command.
3. A VLAN Query Protocol (VQP) port configured with the **switchport access vlan dynamic** interface configuration command.
4. The switch must be running the enhanced software image (EI).
5. You must set the maximum allowed secure addresses on the port to two plus the maximum number of secure addresses allowed on the access VLAN.
6. The switch must be running the enhanced multilayer image (EMI).
7. ARP = Address Resolution Protocol

- (Catalyst 3750 or 3560 switches) When the **show interface** privileged EXEC is entered on a port that is running 802.1Q, inconsistent statistics from ports running 802.1Q might be reported. The workaround is to upgrade to Cisco IOS Release 12.1(20)EA1. (CSCec35100)

- (Catalyst 3750 or 3560 switches) When you change a port from a nonrouted port to a routed port or the reverse, the applied automatic quality of service (auto-QoS) setting is not changed or updated when you verify it by using the **show running interface** or **show mls qos interface** user EXEC commands. These are the workarounds:
  1. Disable auto-QoS on the interface.
  2. Change the routed port to a nonrouted port or the reverse.
  3. Re-enable auto-QoS on the interface. (CSCec44169)
- The DHCP snooping binding database is not written to flash or a remote file in any of these situations:
  - (Catalyst 3750 switch) When the Network Time Protocol (NTP) is configured, but the NTP clock is not synchronized. You can check the clock status by entering the **show NTP status** privileged EXEC command and verifying that the network connection to the NTP server and peer work correctly.
  - (Catalyst 3750, 3560, or 2970 switches) The DHCP snooping database file is manually removed from the file system. After enabling the DHCP snooping database by configuring a database URL, a database file is created. If the file is removed manually from the file system, the DHCP snooping database does not create another database file. You need to disable the DHCP snooping database and enable it again to create the database file.
  - (Catalyst 3750, 3560, or 2970 switches) The URL for the configured DHCP snooping database was replaced because the original URL is not accessible. The new URL might not take effect after the timeout of the old URL.

  No workaround is necessary; these are the designed behaviors. (CSCed50819)
- (Catalyst 3750 or 3560 switches) When dynamic ARP inspection is enabled on a switch or switch stack, ARP and RARP packets greater than 2016 bytes are dropped by the switch or switch stack. This is a hardware limitation.

  However, when dynamic ARP inspection is not enabled and jumbo MTU is configured, ARP and RARP packets are correctly bridged in hardware. (CSCed79734)
- When connected to some third-party devices that send early preambles, a Catalyst 3750 switch port operating at 100 Mbps full duplex or 100 Mbps half duplex might bounce the line protocol up and down. The problem is observed only when the Catalyst 3750 switch is receiving frames.

  The workaround is to configure the port for 10 Mbps and half duplex or to connect a hub or a nonaffected device to the switch. (CSCed390310)

Ethernet

These are the Ethernet limitations:

- Subnetwork Access Protocol (SNAP) encapsulated IP packets are dropped without an error message being reported at the interface. The switch does not support SNAP-encapsulated IP packets. There is no workaround. (CSCdz89142)
- (Catalyst 3750 or 2970 switches) A Gigabit Ethernet connection between a Serial Gigabit Media Independent Interface SGMII) port (3/4, 7/8, 11/12, 15/16, 19/20, and 23/24) and an Intel Pro/1000T Server Adapter NIC might lose connectivity on the Catalyst 3750G-24T and 3750G-24TS switches. The link activates correctly, but might subsequently stop exchanging data. This is an Intel product defect. The workaround is to use Reduced Gigabit Media Independent Interface (RGMII) ports (1/2, 5/6, 9/10, 13/14, 17/18, and 21/22) instead of SGMII ports. You can also use the **speed 1000** interface configuration command to force the speed of the port to 1000 Mbps. (CSCea77032)

Fallback Bridging

These are the fallback bridging limitations:

- (Catalyst 3750 or 3560 switches) If a bridge group contains a VLAN to which a static MAC address is configured, all non-IP traffic in the bridge group with this MAC address destination is sent to all ports in the bridge group. The workaround is to remove the VLAN from the bridge group or to remove the static MAC address from the VLAN. (CSCdw81955)
- (Catalyst 3750 or 3560 switches) Known unicast (secured) addresses are flooded within a bridge group if secure addresses are learned or configured on a port and the VLAN on this port is part of a bridge group. Non-IP traffic destined to the secure addresses is flooded within the bridge group. The workaround is to disable fallback bridging or to disable port security on all ports in all VLANs participating in fallback bridging. To remove an interface from a bridge group and to remove the bridge group, use the **no bridge-group** *bridge-group* interface configuration command. To disable port security on all ports in all VLANs participating in fallback bridging, use the **no switchport port-security** interface configuration command. (CSCdz80499)

HSRP

This is the Hot Standby Routing Protocol (HSRP) limitation:

When the active switch fails in a switch cluster that uses HSRP redundancy, the new active switch might not contain a full cluster member list. The workaround is to ensure that the ports on the standby cluster members are not in the spanning-tree blocking state. To verify that these ports are not in the blocking state, refer to the “Configuring STP” chapter in the software configuration guide. (CSCec76893)

IP

These are the IP limitations:

- (Catalyst 3750 or 3560 switches) The switch does not create an adjacent table entry when the ARP timeout value is 15 seconds and the ARP request times out. The workaround is to not set an ARP timeout value lower than 120 seconds. (CSCea21674)
- When the rate of received DHCP requests exceeds 2,000 packets per minute for a long time, the response time might be slow when you are using the console. The workaround is to use rate limiting on DHCP traffic to prevent a denial of service attack from occurring. (CSCeb59166)
- Some access point (AP)-350 devices are incorrectly discovered as IEEE 802.3af Class 1 devices. These APs should be discovered as Cisco pre-standard devices. The **show power inline** user EXEC command shows the AP-350 as an IEEE Class 1 device. The workaround is to power the AP by using an AC wall adaptor. (CSCin69533)

IP Telephony

These are the IP telephony limitations:

- When a Cisco IP Phone is connected to the switch, the port VLAN ID (PVID) and the voice VLAN ID (VVID) both learn its MAC address. However, after dynamic MAC addresses are deleted, only the VVID relearns the phone MAC address. MAC addresses are manually or automatically deleted when a topology change occurs or when port security or an 802.1x feature is enabled or disabled. There is no workaround. (CSCea80105)
- After you change the access VLAN on a port that has 802.1x enabled, the IP Phone address is removed. Because learning is restricted on 802.1x capable ports, it takes approximately 30 seconds before the address is relearned. No workaround is necessary. (CSCea85312)

MAC Addressing

This is the MAC addressing limitation:

(Catalyst 3750 or 3560 switches) When a MAC address is configured for filtering on the internal VLAN of a routed port, incoming packets from the MAC address to the routed port are not dropped. (CSCeb67937)

Multicasting

These are the multicasting limitations:

- (Catalyst 3750 or 3560 switches) The switch does not support tunnel interfaces for unicast routed traffic. Only Distance Vector Multicast Routing Protocol (DVMRP) tunnel interfaces are supported for multicast routing.
- (Catalyst 3750 or 3560 switches) Nonreverse-path forwarded (RPF) IP multicast traffic to a group that is bridged in a VLAN is leaked onto a trunk port in the VLAN even if the port is not a member of the group in the VLAN, but it is a member of the group in another VLAN. Because unnecessary traffic is sent on the trunk port, it reduces the bandwidth of the port. There is no workaround for this problem because non-RPF traffic is continuous in certain topologies. As long as the trunk port is a member of the group in at least one VLAN, this problem for the non-RPF traffic occurs. (CSCdu25219)
- If the number of multicast routes and Internet Group Management Protocol (IGMP) groups are more than the maximum number specified by the **show sdm prefer** global configuration command, the traffic received on unknown groups is flooded in the received VLAN even though the **show ip igmp snooping multicast-table** privileged EXEC command output shows otherwise. The workaround is to reduce the number of multicast routes and IGMP snooping groups to less than the maximum supported value. (CSCdy09008)
- IGMP filtering is applied to packets that are forwarded through hardware. It is not applied to packets that are forwarded through software. Hence, with multicast routing enabled, the first few packets are sent from a port even when IGMP filtering is set to deny those groups on that port. There is no workaround. (CSCdy82818)
- (Catalyst 3750 or 3560 switches) When you use the **ip access-group** interface configuration command with a router access control list (ACL) to deny access to a group in a VLAN, multicast data to the group that is received in the VLAN is always flooded in the VLAN, regardless of IGMP group membership in the VLAN. This provides reachability to directly connected clients, if any, in

the VLAN. The workaround is to not apply a router ACL set to deny access to a VLAN interface. Apply the security through other means; for example, apply VLAN maps to the VLAN instead of using a router ACL for the group. (CSCdz86110)

- (Catalyst 3750 switch stack) If the stack master is power cycled immediately after the **ip mroute** global configuration command is entered, there is a slight chance that this configuration change might be lost after the stack master changes. This occurs because the stack master did not have time to propagate the running configuration to all the stack members before it was powered down. This problem might also affect other configuration commands. There is no workaround. (CSCea71255)
- (Catalyst 3750 switches) When IP Protocol-Independent Multicast (PIM) is enabled on a tunnel interface, the switch incorrectly displays the `Multicast is not supported on tunnel interfaces` error message. IP PIM is not supported on tunnel interfaces. There is no workaround. (CSCeb75366)
- If an IG MP report packet has two multicast group records, the switch removes or adds interfaces depending on the order of the records in the packet:
  - If the ALLOW_NEW_SOURCE record is before the BLOCK_OLD_SOURCE record, the switch removes the port from the group.
  - If the BLOCK_OLD_SOURCE record is before the ALLOW_NEW_SOURCE record, the switch adds the port to the group.

  There is no workaround. (CSCec20128)
- (Catalyst 3750 switches) Although the **switchport block multicast** interface configuration command appears in the CLI, it is not supported on the Catalyst 3750 switches. There is no workaround. (CSCee16865)

QoS

These are the QoS limitations:

- Some switch queues are disabled if the buffer size or threshold level is set too low with the **mls qos queue-set output** global configuration command. The ratio of buffer size to threshold level should be greater than 10 to avoid disabling the queue. The workaround is to choose compatible buffer sizes and threshold levels. (CSCea76893)
- When auto-QoS is enabled on the switch, priority queuing is not enabled. Instead, the switch uses shaped round robin (SRR) as the queuing mechanism. The auto-QoS feature is designed on each platform based on the feature set and hardware limitations, and the queuing mechanism supported on each platform might be different. There is no workaround. (CSCee22591)

Routing

These are the routing limitations:

- (Catalyst 3750 or 3560 switches) The switch does not support tunnel interfaces for unicast routed traffic. Only Distance Vector Multicast Routing Protocol (DVMRP) tunnel interfaces are supported for multicast routing.
- (Catalyst 3750 or 3560 switches) A route map that has an ACL with a Differentiated Services Code Point (DSCP) clause cannot be applied to a Layer 3 interface. The switch rejects this configuration and displays a message that the route map is unsupported. There is no workaround. (CSCea52915)

- On a Catalyst 3750 switch stack with a large number of switched virtual interfaces (SVIs), routes, or both on a fully populated nine-member switch stack, this message might appear when you reload the switch stack or add a switch to the stack:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of 4252 bytes failed from 0x179C80, alignment 0
  Pool: I/O Free: 77124  Cause: Memory fragmentation
  Alternate Pool: None Free: 0  Cause: No Alternate pool
  ```

  This error message means there is a temporary memory shortage that normally recovers by itself. You can verify that the switch stack has recovered by entering the **show cef line** user EXEC command and verifying that the line card states are `up` and `sync`. No workaround is required because the problem is self-correcting. (CSCea71611)

SPAN and RSPAN

These are the SPAN and Remote SPAN (RSPAN) limitations:

- (Catalyst 3750 or 3560 switches) An egress SPAN copy of routed unicast traffic might show an incorrect destination MAC address on both local and remote SPAN sessions. This limitation does not apply to bridged packets. The workaround for local SPAN is to use the replicate option. For a remote SPAN session, there is no workaround. This is a hardware limitation. (CSCdy72835)
- (Catalyst 3750 or 3560 switches) Egress SPAN routed packets (both unicast and multicast) show the incorrect source MAC address. For remote SPAN packets, the source MAC address should be the MAC address of the egress VLAN, but instead the packet shows the MAC address of the RSPAN VLAN. For local SPAN packets with native encapsulation on the destination port, the packet shows the MAC address of VLAN 1. This problem does not appear with local SPAN when the encapsulation replicate option is used. This limitation does not apply to bridged packets. The workaround is to use the **encapsulate replicate** keywords in the **monitor session** global configuration command. Otherwise, there is no workaround. This is a hardware limitation. (CSCdy81521)
- During periods of very high traffic, when two RSPAN source sessions are configured, the VLAN ID of packets in one RSPAN session might overwrite the VLAN ID of the other RSPAN session. If this occurs, packets intended for one RSPAN VLAN are incorrectly sent to the other RSPAN VLAN. This problem does not affect RSPAN destination sessions. The workaround is to configure only one RSPAN source session. (CSCea72326)
- (Catalyst 3750 or 3560 switches) The egress SPAN data rate might degrade when fallback bridging or multicast routing is enabled. The amount of degradation depends on the processor loading. Typically, the switch can egress SPAN up to 40,000 packets per second (64-byte packets). As long as the total traffic being monitored is below this limit, there is no degradation. However, if the traffic being monitored exceeds the limit, only a portion of the source stream is spanned. When this occurs, the following console message appears: `Decreased egress SPAN rate`. In all cases, normal traffic is not affected; the degradation limits only how much of the original source stream can be egress spanned. If fallback bridging and multicast routing are disabled, egress SPAN is not degraded. There is no workaround. If possible, disable fallback bridging and multicast routing. If possible, use ingress SPAN to observe the same traffic. (CSCeb01216)
- On Catalyst 3750 switches running Cisco IOS Release 12.1(14)EA1 and later and on Catalyst 3560 switches running Cisco IOS release 12.1(19)EA1 or later, some IGMP report and query packets with IP options might not be ingress-spanned. Packets that are susceptible to this problem are IGMP packets containing 4 bytes of IP options (IP header length of 24). An example of such packets would be IGMP reports and queries having the router alert IP option. Ingress-spanning of such packets is not accurate and can vary with the traffic rate. Typically, very few or none of these packets are spanned. There is no workaround. (CSCeb23352)

- Cisco Discovery Protocol (CDP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP) packets received from a SPAN source are not sent to the destination interfaces of a local SPAN session. The workaround is to use the **monitor session** *session_number* **destination** {**interface** *interface-id* **encapsulation replicate**} global configuration command for local SPAN. (CSCed24036)
- (Catalyst 3750 switches)

  A spanning-tree loop might occur if all of these conditions are true:

  - Port security is enabled with the violation mode set to protected.
  - The maximum number of secure addresses is less than the number of switches connected to the port.
  - There is a physical loop in the network through a switch whose MAC address has not been secured, and its BPDUs cause a secure violation.

  The workaround is to change any one of the listed conditions. (CSCed53633)

Stacking (Catalyst 3750 switch stack only)

These are the Catalyst 3750 switch stack limitations:

- If the stack master is immediately reloaded after adding multiple VLANs, the new stack master might fail. The workaround is to wait a few minutes after adding VLANs before reloading the stack master. (CSCea26207)
- If the console speed is changed on a stack, the configuration file is updated, but the baud rate is not. When the switch is reloaded, meaningless characters might appear on the console during bootup before the configuration file is parsed and the console speed is set to the correct value. If manual boot is enabled or the startup configuration is deleted after you change the console speed, you cannot access the console after the switch reboots. There is no workaround. (CSCec36644)
- If a switch is forwarding traffic from a Gigabit ingress interface to a 100 Mbps egress interface, the ingress interface might drop more packets due to oversubscription if the egress interface is on a Fast Ethernet switch (such as a Catalyst 3750-24TS or 3750-48TS switch) than if it is on a Gigabit Ethernet switch (such as a Catalyst 3750G-24T or 3750G-24TS switch). There is no workaround. (CSCed00328)
- If a stack member is removed from a stack and either the configuration is not saved or another switch is added to the stack at the same time, the configuration of the first member switch might be lost. The workaround is to save the stack configuration before removing or replacing any switch in the stack. (CSCed15939)
- When the **switchport** and **no switchport** interface configuration commands are entered more than 20,000 times on a port of a Catalyst 3750 switch, all available memory is used, and the switch halts.

  There is no workaround. (CSCed54150)
- In a private-VLAN domain, only the default private-VLAN IP gateways have sticky ARP enabled. The intermediate Layer 2 switches that have private VLAN enabled disable sticky ARP. When a stack master switch-over occurs on one of the Catalyst 3750 default IP gateways, the message `IP-3-STCKYARPOVR` appears on the consoles of other default IP gateways. Because sticky ARP is not disabled, the MAC address update caused by the stack master switch-over cannot complete.

  The workaround is to complete the MAC address update by entering the **clear arp** privileged EXEC command. (CSCed62409)

- When a Catalyst 3750 switch is being reloaded in a switch stack, packet loss might occur for up to 1 minute while the Cisco Express Forwarding (CEF) table is downloaded to the switch. This only impacts traffic that will be routed through the switch that is being reloaded. There is no workaround. (CSCed70894)
- Inconsistent private-VLAN configuration can occur on a switch stack if a new stack master is running the SMI and the old stack master was running the EMI.

  Private VLAN is enabled or disabled on a switch stack, depending on whether or not the stack master is running the EMI or the SMI:

  – If the stack master is running the EMI, all stack members have private VLAN enabled.
  – If the stack master is running SMI, all stack members have private VLAN disabled.

  This occurs after a master-switchover (MSO) when the previous stack master was running the EMI and the new stack master is running the SMI. The stack members are configured with private VLAN, but any new switch that joins the stack will have private VLAN disabled.

  These are the workarounds. Only one of these is necessary:

  – Reload the stack after an EMI to SMI MSO (or the reverse).
  – Before an EMI-to-SMI MSO, delete the private-VLAN configuration from the existing stack master. (CSCee06802)
- Port configuration information is lost when changing from **switchport** to **no switchport** modes on Catalyst 3750 switches.

  This is the expected behavior of the offline configuration (provisioning) feature. There is no workaround. (CSCee12431)

Trunking

These are the trunking limitations:

- The switch treats frames received with mixed encapsulation (802.1Q and Inter-Switch Link [ISL]) as frames with FCS errors, increments the error counters, and causes the LED to blink amber. This happens when an ISL-unaware device receives an ISL-encapsulated packet and forwards the frame to an 802.1Q trunk interface. There is no workaround. (CSCdz33708)
- IP traffic with IP options set is sometimes leaked on a trunk port. For example, a trunk port is a member of an IP multicast group in VLAN X but is not a member in VLAN Y. If VLAN Y is the output interface for the multicast route entry assigned to the multicast group and an interface in VLAN Y belongs to the same multicast group, the IP-option traffic received on an input VLAN interface other than one in VLAN Y is sent on the trunk port in VLAN Y because the trunk port is forwarding in VLAN Y, even though the port has no group membership in VLAN Y. There is no workaround. (CSCdz42909).
- If a Catalyst 3750 switch stack is connected to a designated bridge and the root port of the switch stack is on a different switch than the alternate root port, changing the port priority of the designated ports on the designated bridge has no effect on the root port selection for the Catalyst 3750 switch stack. There is no workaround. (CSCea40988)
- For trunk ports or access ports configured with 802.1Q tagging, inconsistent statistics might appear in the **show interfaces counters** privileged EXEC command output. Valid 802.1Q frames of 64 to 66 bytes are correctly forwarded even though the port LED blinks amber, and the frames are not counted on the interface statistics. There is no workaround. (CSCec35100).

VLAN

This is the VLAN limitation:

If the number of VLANs times the number of trunk ports exceeds the recommended limit of 13,000, the switch can fail. The workaround is to reduce the number of VLANs or trunks. (CSCeb31087)

Cluster Limitations and Restrictions

These limitations apply to the Catalyst 3750, 3560, and 2970 switches:

- When there is a transition from the cluster active command switch to the standby command switch, Catalyst 1900, 2820, and 2900 4-MB switches that are cluster members might lose their cluster configuration. You must manually add these switches back to the cluster. (CSCds32517 and CSCds55711)
- When a Catalyst 2900 XL or 3500 XL cluster command switch is connected to a Catalyst 3550 or to a 3750 switch, the command switch does not find any cluster candidates beyond the Catalyst 3550 or the 3750 switch if it is not a member of the cluster. You must add the Catalyst 3550 or the 3750 switch to the cluster. You can then see any cluster candidates connected to it. (CSCdt09918)
- If both the active command switch and the standby command switch fail at the same time, the cluster is not automatically recreated. Even if there is a third passive command switch, it might not recreate all cluster members because it might not have all the latest cluster configuration information. You must manually recreate the cluster if both the active and standby command switches simultaneously fail. (CSCdt43501)

CMS Limitations and Restrictions

These limitations apply to the Catalyst 3750, 3560, and 2970 switches:

- The device manager **Launch** button does not work for Catalyst 1900 and 2820 switches. The workaround is to launch device manager for these devices outside of CMS by opening a new browser and manually entering the URL for the switch. (CSCee15761)
- CMS performance degrades if the Topology View is open for several hours on a Solaris machine. The cause might be a memory leak.The workaround is to close the browser, reopen it, and launch CMS again. (CSCds29230)
- If you are printing a Topology View or Front Panel View that contains many devices and are running Solaris 2.6 with JDK1.2.2, you might get an *Out of Memory* error message. The workaround is to close the browser, re-open it, and launch CMS again. Before you perform any other task, open the view that you want to print, and click Print in the CMS menu. (CSCds80920)
- A red border appears around the text-entering area of some CMS dialogs. The color of the border changes to green when text is entered. This is only a cosmetic error. The colored border does not prevent you from entering text. (CSCdv82352)
- You cannot switch modes (for example, from Guide Mode to Expert Mode) for an open CMS window. The workaround is to close the open window, select the mode that you want, and then reopen the CMS window. For the mode change to take effect on any other CMS window that is open, you need to close that window and then reopen it after you select the new mode. (CSCdw87550)
- If you open a window in which you can enter text, open another window, and return to the first window, right-clicking in the text field might make the cursor in this field disappear. You can still enter text in the field. (CSCdy44189)

- CMS fails when a switch is running the cryptographic software image and the vty lines have been configured to use only SSH using the **transport input ssh** and **line vty 0 15** global configuration commands. The workaround is to allow SSH and Telnet access through the vty lines by using the **transport input ssh telnet** and **line vty 0 15** global configuration command. (CSCdz01037)
- When you add a new member with a username and password that is different from the existing cluster member usernames and passwords, CMS produces an exception error because of an authentication failure. The workaround is to add the new member without any username and password. When the new member is added to the cluster, remove the existing username and password from the Username and Password fields, enter a new username and password, and then apply it to all cluster members. (CSCdz07957)
- When the Link Graphs application has run for hours displaying packet drop and error information, sometimes the X-axis crosses the Y-axis at a negative y value instead of at y = 0. This condition occurs with all supported operating systems, browsers, and Java plug-ins. There is no workaround. (CSCdz32584)
- After you click **Apply** or **Refresh** in the Simple Network Management Protocol (SNMP) window, the window size changes. (CSCdz75666, CSCdz84255)
- When you enable log scaling for Link Graphs, the Y-axis scale becomes illegible. There is no workaround. (CSCdz81086)
- The CMS window does not return to full size after resizing the browser when you are using Netscape version 6.xx on Solaris and Linux. This is a Netscape browser problem. There is no workaround. (CSCea01179)
- CMS sometimes halts after you click **Apply** when using Netscape 4.7 on the Japanese version of Windows 98 or Windows ME. The workaround is to use Microsoft Internet Explorer or Netscape 6.0 or later. (CSCea27408)
- Changing the password or current authentication while CMS is running causes HTTP requests to fail. The workaround is to close all browser sessions and then relaunch CMS. (CSCeb33995)
- The CMS plug-in is not supported in Netscape 4.7x. The workaround is to use a supported browser, such as Netscape 7.1 or Internet Explorer 5.5 or 6.0. (CSCed21655)
- When TACACS authentication is only enabled on a command switch, member switches cannot be configured. The workaround is to enable TACACS authentication on the member switches. (CSCed27723)
- If an ACL is deleted from a device, all QoS classes that use this ACL for traffic classification become unusable (only on Catalyst 2970 and 3750 switches). The modification of these classes to use any other traffic classification (match statement) fails. The workaround is to delete the QoS class that uses the undefined ACL and then recreate it with the intended traffic classification (match statement). (CSCed40866)
- When an Open Shortest Path First (OSPF) summary address is added for a 10.x.x.x network, a Windows exception error sometimes occurs.

  The workaround is to add the address by using the **router ospf** <*process-id*>, **area** <*area-id*>, and **range** <*address*> <*mask*> configuration commands. (CSCed87031)
- The Telnet link on the TOOLS page (select TOOLS from the switch home page) does not work on Solaris systems.

  There is no workaround. (CSCee11710)
- A Java exception error occurs when CMS is in read-only mode and you launch the Port Settings dialog. This only occurs on Catalyst 2900 XL, 3500 XL, and 2950 LRE switches.

  The workaround is to open the Port Settings dialog with CMS in read-write mode. (CSCee25870)

- Host names and Domain Name System (DNS) server names that contain commas on a cluster command switch, member switch, or candidate switch can cause CMS to behave unexpectedly. You can avoid this instability in the interface by not using commas in host names or DNS names. Do not enter commas when also entering multiple DNS names in the IP Configuration tab of the IP Management window in CMS.
- Access control entries (ACEs) that contain the **host** keyword precede all other ACEs in standard ACLs. You can reposition the ACEs in a standard ACL with one restriction: No ACE with the **any** keyword or a wildcard mask can precede an ACE with the **host** keyword.

Important Notes

These sections describe the important notes related to this software release for the Catalyst 3750, 3560, and 2970 switches:

- "Switch Stack Notes" section on page 21
- "Cisco IOS Notes" section on page 21
- "CMS Notes" section on page 22

Switch Stack Notes

These notes apply to switch stacks:

- Always power off a switch before adding or removing it from a switch stack.
- The Catalyst 3560 and 2970 switches do not support switch stacking. However, the **show processes** privileged EXEC command still lists stack-related processes. This occurs because these switches share common code with other switches that do support stacking.

Cisco IOS Notes

These notes apply to Cisco IOS software:

- The 802.1x feature in Cisco IOS Release 12.1(14)EA1 and later is not fully backward-compatible with the same feature in Cisco IOS Release 12.1(11)AX. If you are upgrading a Catalyst 3750 or a 2970 switch running Cisco IOS Release 12.1(11)AX that has 802.1x configured, you must re-enable 802.1x after the upgrade by using the **dot1x system-auth-control** global configuration command. This global command does not exist in Cisco IOS Release 12.1(11)AX. Failure to re-enable 802.1x weakens security because some hosts can then access the network without authentication.
- The behavior of the **no logging on** global configuration command changed in Cisco IOS Release 12.2(18)SE and later. In Cisco IOS Release 12.1(19)EA and earlier, both of these command pairs disabled logging to the console:
  - the **no logging on** and then the **no logging console** global configuration commands
  - the **logging on** and then the **no logging console** global configuration commands

  In Cisco IOS Release 12.2(18)SE and later, you can only use the **logging on** and then the **no logging console** global configuration commands to disable logging to the console. (CSCec71490)

CMS Notes

These notes apply to CMS configuration:

- If you use CMS on Windows 2000, it might not apply configuration changes if the enable password is changed from the CLI during your CMS session. You have to restart CMS and enter the new password when prompted. Platforms other than Windows 2000 prompt you for the new enable password when it is changed.
- CMS does not display QoS classes that are created through the CLI if these classes have multiple match statements. When using CMS, you cannot create classes that match more than one match statement. CMS does not display policies that have such classes.
- If you use Internet Explorer Version 5.5 and select a URL with a nonstandard port at the end of the address (for example, *www.cisco.com*:84), you must enter *http://* as the URL prefix. Otherwise, you cannot launch CMS.
- Within an ACL, you can change the sequence of ACEs that have the **host** keyword. However, because such ACEs are independent of each other, the change has no effect on the way the ACL filters traffic.
- If you have a proxy server configured on your web browser, CMS can run slowly and take 2 to 3 minutes to process each command that is entered.
- If you use the Netscape browser to view the CMS GUI and you resize the browser window while CMS is initializing, CMS does not resize to fit the window.

  The workaround is to resize the browser window again when CMS is not busy.
- In the Front Panel view or Topology view, CMS does not display error messages in read-only mode for these switches:
  - Catalyst 2900 XL or Catalyst 3500 XL member switches running Cisco IOS Release 12.0(5)WC2 or earlier
  - Catalyst 2950 member switches running Cisco IOS Release 12.0(5)WC2 or earlier
  - Catalyst 3550 member switches running Cisco IOS Release 12.1(6)EA1 or earlier

  In the Front Panel view, if the switch is running one of the software releases listed previously, the device LEDs do not appear. In Topology view, if the member is an LRE switch, the CPE devices that are connected to the switch do not appear. The Bandwidth and Link graphs also do not appear in these views.

Open Caveats

These sections describe the open caveats with possible unexpected activity in this software release:

- "Open Cisco IOS Caveats" section on page 23
- "Open CMS Caveats" section on page 28

Open Cisco IOS Caveats

Unless otherwise noted, these severity 3 Cisco IOS configuration caveats apply to the Catalyst 3750, 3560, and 2970 switches:

- CSCeb35422

  When both 802.1x and port security are enabled on a voice VLAN port, dynamic secure addresses might not be cleared when the port changes from multihosts mode to single-host mode under these conditions:

  - The port is in the authorized state.
  - Multiple hosts were learned on the port before the mode change.
  - VLAN assignment is not enabled for the authorized host.

  MAC addresses that were learned before mode change (when the port was in multihosts mode) are still allowed, even though the port is now in single-host mode.

  The workaround is to disable and re-enable port security on the port.

- CSCeb42949 (Catalyst 3750 switches)

  A Catalyst 3750 switch does not work with the User Registration Tool (URT). The PC attempting to connect to the network can log in successfully, but it is not allowed to pass traffic after the port is moved to the user VLAN. The MAC address for that device shows *BLOCKED*.

  There is no workaround.

- CSCec68807 (Catalyst 3750 switches)

  Memory allocation (malloc) and remote-procedure call (RPC) throttle messages sometimes appear when a large number of access control lists (ACLs) are pasted to the console window.

  The workaround is to save the configuration and reload the switch stack.

- CSCec88895 (Catalyst 3750 switches)

  There is a discrepancy between the output of the **show controllers ethernet-controller tengigabitethernet1/0/1** and the **show interfaces tengigabitethernet1/0/1** privileged EXEC commands on a 10-Gigabit Ethernet interface.

  The workaround for 10-Gigabit Ethernet interfaces is to use the **show interface** privileged EXEC command for the byte count and the number of pause frames received. Use the **show controllers ethernet-controller** privileged EXEC command for the frame count and the FCS and CRC error-frame count.

- CSCed12889 (Catalyst 3750 switches)

  When redundant uplinks are from the same stack member in a switch stack and UplinkFast is configured, dummy multicast packets are not sent.

  The workaround is to not have redundant uplinks from the same stack member. Provide uplink connectivity from ports across the switch stack rather than from one switch in the stack.

- CSCed65309 (Catalyst 3750 or 3560 switches)

  Some invalid ARP packets are not dropped on dynamic ARP inspection-enabled VLANs. Dynamic ARP inspection does not verify that certain ARP fields are valid and does not drop ARP packets with invalid values for those fields. The fields are hardware size, protocol size, and operation type. These packets also are not dropped by the switch on nondynamic ARP-enabled VLANs.

  There is no workaround.

- CSCed65410 (Catalyst 3750 or 3560 switches)

  If dynamic ARP inspection is enabled on an internal VLAN used by a routed port, ARP traffic on the routed port is affected by the dynamic ARP inspection processing. For example, ARP packets will be rate-limited.

  The workaround is to not enable dynamic ARP inspection on internal VLANs.

- CSCed74349 (Catalyst 3750 switches)

  An EtherChannel is not properly error-disabled if these conditions are true:

  - The channel is carrying a VLAN that is enabled for dynamic ARP inspection.
  - The channel is configured with a rate limit for dynamic ARP inspection.
  - At least one of the ports in the channel is on a stack member.
  - ARP packets are received on a port in the channel on a stack member *at a higher rate* than the configured rate limit for the channel.

  Under these circumstances, a system message states that the rate limit was exceeded on the channel, but the channel will not be error-disabled.

  The workaround is to use physical ports on the stack master for any EtherChannel that carries dynamic ARP inspection VLANs and has rate limits.

- CSCed87243

  If the VTP password is configured but the VTP domain name is not configured and if the switch reloads twice, the switch does not retain the VLAN information.

  Use of these workarounds:

  - Delete the vlan.dat file, which deletes the VTP password.
  - Delete the VTP password by using the **no vtp password** global configuration command.
  - Assign a VTP domain name.

- CSCed91730 (Catalyst 3750 switches)

  When a secondary VLAN is associated and then quickly disassociated, sometimes the MAC address tables across the switch stack become unsynchronized. This is a rare condition that happens when Port Fast is enabled on the host ports and traffic is continuously received on that port.

  The workaround is to clear the MAC address table by using the **clear mac address-table dynamic** privileged EXEC command.

- CSCed94657 (Catalyst 3750 or 3560 switches)

  If a secondary VLAN that was mapped to a promiscuous port is disassociated from the primary VLAN, the LED on the port turns from green to amber. This also occurs if the secondary VLAN is deleted.

  The workaround is to remove the secondary VLAN from the mapping of the promiscuous port.

- CSCed95822 (Catalyst 3750 switches)

  Dynamic ARP inspection log entries might be lost after a switch failure. Any log entries that are still in the log buffer (have not been output as a system message) on a switch that fails will be lost.

  When you enter the **show ip arp inspection log** privileged EXEC command, the log entries from all switches in the stack are moved to the switch on which the command was entered.

  There is no workaround.

- CSCee07107 (Catalyst 3750 switches)

  ARP and reverse ARP (RARP) packets are not properly filtered by a configured VLAN map. If you enable a VLAN for dynamic ARP inspection and a VLAN map is applied to the VLAN, ARP and RARP packets received in that VLAN on stack member ports that should be dropped by the VLAN map are not dropped.

  There is no workaround.

- CSCee08756

  Configuring multiple ports to a static address in a private VLAN is not supported in this release. If you add more than one port to a static address in a private VLAN, the traffic destined to that static address from a host (secondary VLAN) port to promiscuous port might be dropped.

  The workaround is to not configure multiple ports to a static address in a private VLAN. You can use the **shutdown** and **no shutdown** interface configuration commands on a promiscuous port to resume the flow of traffic.

- CSCee11197 (Catalyst 3750 switches)

  You can only enter values ranging from 1 to 1023 when configuring the VLAN for an access port from SNMP by using the vlanPortVlan object of the CISCO-STACK-MIB.

  These are the workarounds:

  - Use the **interface vlan** global configuration command to configure the VLAN for the access port.
  - From SNMP, use the vmVlan object of the CISCO-VLAN-MEMBERSHIP-MIB.

  You can use both of these workarounds to enter a value ranging from 1 to 4095.

- CSCee14018 (Catalyst 3750 or 3560 switches)

  Port ACLs are not applied to IGMP control packets with IP options.

  There is no workaround.

- CSCee14293 (Catalyst 3750 or 3560 switches)

  After a multicast group exceeds the maximum number that a private VLAN can support, the required ternary content addressable memory (TCAM) entries cannot present for the last group, and the forwarding behavior for that multicast group is incorrect.

  For a private VLAN multicast group, each group needs 3 TCAM entries (one SFT entry and 2 LFT entries) when IP multicast routing is enabled on the private VLAN primary VLAN. (For a regular VLAN, only 1 SFT TCAM entry is required, and approximately1000 groups can be supported. For the private VLAN group, only one third of the regular groups can be supported.

  There is no workaround.

- CSCee14673 (Catalyst 3750 switches)

  A Catalyst 3750 switch running Cisco IOS Release 12.1(19)EA1a might continuously show this message:

  ```
  %LINK-3-BADMACREG: Interface StackPort1, non-existent MACADDR registry for link 0
  -Process= “<interrupt level>”, ipl= 4-Traceback= 20AC84 188828 58ACCC 588F20 2D8020
  2E00B4 2E2B80 2E2EAC 2B14E8
  ```

  There is no workaround.

- CSCee22376

  When an SNMP version 3 user is configured with the encrypted option and password, the switch reloads when the MIB object usmUserAuthKeyChange is set.

  The workaround is to configure a user without the encrypted option. (For example, **snmp-server user username groupname v3 auth md5 password**.)

- CSCee30022

  If you try to add an aggregate policer to a policy map, this message appears:

  ```
  BAD policymap info 9999999
  ```

  and the aggregate policer is not added.

  The workaround is to delete the policy map by using the **no policy-map** *policy-map-name* global configuration command, recreate it with the desired configuration, and then re-attach it to the interfaces by using the **service-policy input** *policy-map-name* interface configuration command.

- CSCee30090

  If you modify a policer, this message appears:

  ```
  Download failed for <class-name>
  ```

  If you then attempt to remove an aggregate policer, the removal of the policy map fails, and this message appears:

  ```
  Bad policymap info.
  ```

  The workaround is to delete the policy map by using the **no policy-map** *policy-map-name* global configuration command, recreate it with the desired configuration, and then re-attach it to the interfaces by using the **service-policy input** *policy-map-name* interface configuration command.

- CSCee30129

  When you add an aggregate policer to a policy-map class, the aggregate policer is also added to another policy class within the same policy.

  The workaround is to delete the policy map by using the **no policy-map** *policy-map-name* global configuration command, recreate it with the desired configuration, and then re-attach it to the interfaces by using the **service-policy input** *policy-map-name* interface configuration command.

- CSCee41566 (Catalyst 3750 switches)

  Auto-upgrade fails under either of these conditions:

  - The stack is running a cryptographic image and a version-mismatch member switch that is running a non-cryptographic image of the same type (both are EMI or SMI) joins the stack, or the reverse.
  - If the stack is running a Cisco IOS 12.1 crypto image and a member switch running a Cisco IOS 12.2 crypto image of the same type joins the stack, or the reverse.

  In both cases, the newly added member switch remains in the version mismatch state, and you must manually upgrade the member switch to run a compatible Cisco IOS image.

  The workaround is to remove the 3750 member switch from the switch stack and to load a cryptographic image on the switch before adding it to the stack.

- CSCee53804 (Catalyst 3750 or 3560 switches)

  When enabled, DHCP snooping does not work with secondary VLANs of a private VLAN. DHCP discover messages from the private-VLAN hosts are not broadcast, and private-VLAN hosts cannot communicate with the DHCP server.

  There is no workaround.

- CSCee75231 (Catalyst 3750-G12S switches)

  You cannot use the Mode button to detect the presence of a switch stack member if a small form-factor (SFP) module is not in the module slot for that port on the member.

  The workaround is to insert an SFP module into the port.

- CSCee75389 (Catalyst 3750 switches)

  When you reload a stack master, the SFP module slots are unable to establish a link after the old stack master comes up as a member switch.

  The workaround is to manually configure the port by entering the **no speed nonegotiate**, **shut**, and **no shut** interface configuration commands.

- CSCee88546 (Catalyst 3750 switches)

  After a stack master fail-over, any per-user access control lists (ACLs) applied on authenticated 802.1x ports might appear twice when you enter the **show ip access-list** privileged EXEC command.

  This occurs when the authenticated port is on a member switch that becomes the stack master during fail-over. The duplicate display does not affect the functional behavior of the ACL.

  There is no workaround.

- CSCee89040 (Catalyst 3750 switches)

  When a local network link comes up, a MAC address that is defined in the static ARP table does not install the adjacency table immediately, causing a temporary Cisco Express Forwarding (CEF) drop. The maximum installation delay is about 60 seconds.

  There is no workaround.

- CSCin68965 (Catalyst 3750 or 3560 switches)

  When two ports of a Cisco IP Phone are connected to a switch and the higher voice VLAN ID (VVID) is configured on the switch port to which port P3 of the Cisco IP Phone is connected, the phone displays *configuring IP* and halts.

  These are the workarounds. Only one of these is necessary:

  - Configure the higher VVID on port P1 of the Cisco IP phone.
  - Connect only one port of the Cisco IP Phone to the switch.

Open CMS Caveats

Unless otherwise noted, these severity 3 CMS caveats apply to the Catalyst 3750, 3560, and 2970 switches:

- CSCee06206

  When a Catalyst 3750 stack member leaves or joins the switch stack, the entire stack disappears from the Topology View. Only the stack member that has left the stack should disappear from the Topology view.

  There is no workaround.

- CSCee26671

  When you click **Refresh** in the Stack Settings dialog, the latest information for the switch cluster does not appear.

  The workaround is to close and then to reopen the Stack Settings dialog.

Resolved Caveats

These are the caveats that have been resolved.

- "Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(20)SE3" section on page 28
- "Cisco IOS Caveat Resolved in Cisco IOS Release 12.2(20)SE2" section on page 31
- "Cisco CMS Caveats Resolved in Cisco IOS Release 12.2(20)SE1" section on page 32
- "Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(20)SE" section on page 32
- "Cisco CMS Caveats Resolved in Cisco IOS Release 12.2(20)SE" section on page 34

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(20)SE3

Unless otherwise noted, these caveats were resolved in this release for the Catalyst 3750, 3560, and 2970 switches:

- CSCed78149

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

- CSCee67450 (Catalyst 3750 and 3560)

  A Cisco device running Cisco IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DoS) attack from a malformed BGP packet. Only devices with the command **bgp log-neighbor-changes** configured are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

  If a misformed packet is received and queued up on the interface, this bug may also be triggered by other means which are not considered remotely exploitable such as the use of the command **show ip bgp neighbors** or running the command **debug ip bgp** *neighbor* **updates** for a configured bgp neighbor.

  Cisco has made free software available to address this problem.

  For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml

- CSCef35924 (Catalyst 3750 and 3560)

  The switch no longer experiences memory leak during the IP Routing Information Base (RIB) update process.

- CSCef37743 (Catalyst 3750 and 3560)

  A switch no longer reloads if it generates a large number of proxy ARP entries.

- CSCef78081 (Catalyst 3750 and 3560)

  If a connected device sends a SNAP Address Resolution Protocol (ARP) request to a switch, communication no longer stops between the devices.

- CSCef68246 (Catalyst 3750)

  The switch no longer reloads when you disable the 802.1x feature by using the **no dot1x system-auth-control** global configuration command on the master switch.

- CSCef55486

  A switch configured for 802.1x accounting no longer reloads after losing connectivity to the RADIUS server.

- CSCee87655

  During 802.1x machine authentication, the switch no longer prompts the supplicant to authenticate twice.

- CSCef97610 (Catalyst 3750 and 3560)

  If an interface on a switch is configured with the **no switchport** interface configuration command, you can now use SNMP with the MIB object ipNetToMediaTable to create an ARP table for the interface information.

- CSCea90941 (Catalyst 3750 and 3560)

  The Enhanced Interior Gateway Routing Protocol (EIGRP) Stub Routing feature is no longer missing from the switch configuration when it is restarted.

- CSCed16920

  High CPU utilization no longer occurs on a switch when the **logging synchronous** global configuration command is configured for **line con 0**.

- CSCef59879

  When a switch is configured for 802.1x authentication and a large number of authentication requests are received in a short period of time, new devices can now authenticate.

- CSCef74348

  The switch now sends EAPOL-Id-Request frames to supplicants after the 802.1x state machine moves to the DISCONNECTING state.

- CSCef27245 (Catalyst 3750 and 3560)

  If a switch stack is load balanced through two trunk uplinks, and one of the uplinks goes down, the packets are no longer forwarded to the wrong VLAN upon recovery of the failed uplink.

- CSCef61682

  Incomplete ARP entries are no longer created when a switch receives an ARP request and sends a reply by using proxy ARP.

- CSCef39372

  A switch no longer sends out an EAP success frame before assigning a corresponding VLAN on a port.

- CSCef42734

  An 802.1x client no longer fails to authenticate on a switch when State(24) Field values change from Challenge to Request.

- CSCee06965

  A switch configured for 802.1x authentication no longer fails to authenticate supplicants because no AAA process slots are available.

- CSCee50294

  Cisco IOS® devices running branches of Cisco IOS version 12.2S that have Dynamic Host Configuration Protocol (DHCP) server or relay agent enabled, even if not configured, are vulnerable to a denial of service where the input queue becomes blocked when receiving specifically crafted DHCP packets. Cisco is providing free fixed software to address this issue. There are also workarounds to mitigate this vulnerability. This issue was introduced by the fix included in CSCdx46180 and is being tracked by Cisco Bug ID CSCee50294.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20041110-dhcp.shtml

Cisco IOS Caveat Resolved in Cisco IOS Release 12.2(20)SE2

This caveat was resolved in this release:

- CSCef23660

This error message no longer appears, and the switch no longer and loops indefinitely after you upgrade and then reload a Catalyst 3750 switch:

```
Unexpected exception to CPUvector 700, PC = 24B634
```

Note There is no code change in Cisco IOS Release 12.2(20)SE2. The SMI cryptographic images on CCO for Cisco IOS Release 12.2(20)SE1 were corrupt. If you have downloaded a corrupted image and are seeing this error message, refer to the "Recovering from Corrupted Software By Using the Xmodem Protocol" section of the software configuration guide at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/12220se/3750scg/swtrbl.htm#wp1099467

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(20)SE1

Unless otherwise noted, these caveats were resolved in this release for the Catalyst 3750, 3560, and 2970 switches:

- CSCec84254

  Catalyst switches running Cisco IOS Release 12.1(14)EA1 through 12.1(19)EA1d or Cisco IOS Release 12.2(18)SE through 12.2(20)SE now correctly link up with media converters running at 100 Mbps.

- CSCed46277 (Catalyst 3750 switches)

  After the stack master fails and another is elected, switch ports on the new stack master no longer lose the hardware configuration of 802.1x per-user access control lists (ACLs).

- CSCed63521 (Catalyst 3750 switches)

  A Catalyst 3750 stack member switch now reliably downloads CEF tables from the stack master.

- CSCee11587 (Catalyst 3750 switches)

  These CISCO-STACK-MIB objects now return the correct values:

  - vlanPortSwitchLevel
  - vlanPortIslAdminStatus
  - vlanPortIslOperStatus
  - vlanPortAdminStatus

- CSCee89456 (Catalyst 3750-PWR and 3560 switches)

  Power is no longer applied to a port after a Power over Ethernet (PoE) switch powered device, such as a Cisco IP Phone, is removed from that port. In previous releases, power was sometimes still applied to the port even after the device was removed. This could have damaged a non-PoE switch-powered device when it was later connected to that port.

Cisco CMS Caveats Resolved in Cisco IOS Release 12.2(20)SE1

Unless otherwise noted, these caveats were resolved in this release for the Catalyst 3750, 3560, and 2970 switches:

- CSCee26637

  When you open the Port Settings dialog for a Power-over-Ethernet (PoE) switch that is a member of a switch stack and the stack master is not a PoE switch, a Java exception error no longer occurs.

- CSCec61919

  When a switch cluster has only one member switch and that member switch is down, CMS now displays the **Remove From Cluster** option.

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(20)SE

Unless otherwise noted, these caveats were resolved in this release for the Catalyst 3750, 3560, and 2970 switches:

- CSCdz30046 (Catalyst 3560 switches)

  When multicast VLAN registration (MVR) groups are added or deleted, the receiver port that joined the groups after the addition no longer receives traffic after the group is deleted. MVR data traffic to the group is no longer sent to the receiver port immediately after the **no mvr group** *ip-address* global configuration command is entered.

- CSCeb67510

  When both the sharing and shaping weights are enabled, the receiving rates now follow the shared bandwidth weight if the priority queue is enabled on the egress queue.

- CSCec07637 (Catalyst 3560 switches)

  When an ACL that denies packets is configured on an ingress or egress interface, the CPU usage is no longer as high as 70 percent when these packets are forwarded to the CPU to determine if an ICMP-unreachable packet should be generated.

- CSCec11048 (Catalyst 3560 switches)

  When a configured secure MAC address exists on an interface, you can now change it to a sticky MAC address. Alternatively, if a sticky MAC address exists on an interface, you can now change it to a secure MAC address.

- CSCec12147 (Catalyst 3560 switches)

  When the CISCO-STP-EXTENSIONS-MIB is polled, unknown indexes are no longer returned for some MIB objects.

- CSCec16481 (Catalyst 3750 or 3560 switches)

  A Cisco device running Internetwork Operating System (IOS) and enabled for the Open Shortest Path First (OSPF) Protocol is vulnerable to a Denial of Service (DoS) attack from a malformed OSPF packet. The OSPF protocol is not enabled by default.

  The vulnerability is only present in IOS release trains based on 12.0S, 12.2, and 12.3. Releases based on 12.0, 12.1 mainlines and all IOS images prior to 12.0 are not affected. Refer to the Security Advisory for a complete list of affected release trains.

  Further details and the workarounds to mitigate the effects are explained in the Security Advisory which is available at the following URL:
  http://www.cisco.com/warp/public/707/cisco-sa-20040818-ospf.shtml

- CSCec21040 (Catalyst 3560 switches)

  When an 802.1x-enabled port is authenticated with a RADIUS-assigned VLAN, if the port is shut down or the link is removed, a traceback message no longer appears.

- CSCec21320 (Catalyst 3560 switches)

  After a link is up, a switch sends three Extensible Authentication Protocol (EAP) Request/Identity messages to the client. There is a 30-second gap between messages. However, PCs that are running Windows XP or Windows 2000 drop the first message so that the second message that the client receives *appears* to be the first, which is at least 30 seconds after the link is up. Therefore, a user does not see a password window until at least 30 seconds after the link is up.

- CSCec22431 (Catalyst 3560 switches)

  Telnet and ping traffic is no longer disrupted during SNMP polling of the VlanTrunkPortTable table in the CISCO-VTP-MIB.

- CSCec22572 (Catalyst 3560 switches)

  When per-user access control lists (ACLs) are downloaded from a RADIUS server after successful 802.1x authentication, disabling 802.1x now removes the attached per-user ACLs from the interface.

- CSCec27421 (Catalyst 3560 switches)

  If QoS is enabled and the trust state is not configured on an ingress interface, now only the mapping of the class of service (CoS) value of 0 to the ingress or egress queues takes effect when you enter the **mls qos srr-queue input cos-map** or the **mls qos srr-queue output cos-map** global configuration command. Other CoS values DSCP values to queue mapping have no effect on traffic from that interface.

- CSCec29970 (Catalyst 3560 switches)

  If you change the input priority queue for queue 2 by using the **mls qos srr-queue input priority-queue 2 bandwidth** global configuration command, the configurations that are generated no longer contain an extra **input** keyword such as **mls qos srr-queue input priority-queue input 2 bandwidth**. In previous releases, the extra keyword caused an error message if the command was saved and the switch was reloaded.

- CSCec31436 (Catalyst 3560 switches)

  When there are many configured secure and sticky MAC addresses on a port, addresses are no longer dropped and removed from the configuration when the switch restarts.

- CSCec32453 (Catalyst 3560 switches)

  When you configure a unicast MAC address filter that matches a Windows XP 802.1x client MAC address, the Windows XP 802.1x client now no longer repeatedly tries to re-authenticate itself.

- CSCec35148 (Catalyst 3560 switches)

  Processor memory no longer leaks if you change the policy-based routing (PBR) configuration.

- CSCec89120 (Catalyst 3750 or 3560 switches)

  The command switch now discovers candidates more than one CDP hop beyond its routed port.

- CSCed04063

  When the **kerberos clients mandatory** global configuration command is entered on a switch and the switch is connected to a host that does not support Kerberos through a Telnet session, the switch no longer halts when the you press the Enter key.

- CSCed18488 (Catalyst 3750 or 3560 switches)

  When (*,G) and (S,G) entries are created in a multicast routing table on a remote port by Protocol-Independent Multicast-Sparse Mode (PIM-SM) registering, the RPF leak flag is now set for hardware entry for the group.

- CSCed30095 (Catalyst 3750 switches)

  A topology change on a member switch no longer causes fast-aging of the dynamically learned addresses. In previous releases, this occurred in per-VLAN spanning-tree (PVST) mode when a topology change notification (TCN BPDU) was generated and propagated from a member switch but was not sent from the root port on the master.

- CSCed33792 (Catalyst 3750 switches)

  Members of a switch stack no longer fail after the **debug all** privileged EXEC command is entered.

- CSCed34921 (Catalyst 3750 switches)

  Changing the LACP system-priority, either locally or on the neighbor switch, no longer creates assert failure and traceback error messages for the ports in the EtherChannel if there is a Layer-3 (routed port) Link Aggregation Control Protocol (LACP) EtherChannel on the stack master,

- CSCed54175 (Catalyst 3750 or 3560 switches)

  The switch now accepts duplicate remark statements in named ACLs.

- CSCee02006 (Catalyst 3750 switches)

  A Catalyst 3750 stack member switch no longer reloads or displays a message similar to this:

  ```
  Unexpected exception to CPUvector 2000, PC = B41D34
  ```

  A MAC address is now correctly learned on a secure port, ages out, and is then learned on another secure port on a different stack member switch.

Cisco CMS Caveats Resolved in Cisco IOS Release 12.2(20)SE

Unless otherwise noted, these caveats were resolved in this release for the Catalyst 3750, 3560, and 2970 switches:

- CSCee26637

  When you open the Port Settings dialog for a Power-over-Ethernet (PoE) switch that is a member of a switch stack and the stack master is not a PoE switch, a Java exception error no longer occurs.

- CSCec61919

  When a switch cluster has only one member switch and that member switch is down, CMS now displays the **Remove From Cluster** option.

Documentation Updates

These are the updates to the product documentation:

- "Documentation Updates for Catalyst 3750 Switches Running Cisco IOS Release 12.2(20)SE3" section on page 35
- "Documentation Updates for Catalyst 3560 Switches Running Cisco IOS Release 12.2(20)SE3" section on page 45

- "Documentation Updates for Cisco IOS Release 12.2(20)SE1" section on page 53
- "Documentation Updates for Cisco IOS Release 12.2(20)SE" section on page 59

Documentation Updates for Catalyst 3750 Switches Running Cisco IOS Release 12.2(20)SE3

The following commands are supported on the Catalyst 3750G-24TS-1U, 3750G-24PS, 3750G-48TS, and 3750G-48PS switches and will be included in the next version of the Catalyst 3750 command reference.

debug platform frontend-controller

Use the **debug platform frontend-controller** privileged EXEC command to enable debugging of front-end controller activity. Use the **no** form of this command to disable debugging.

debug platform frontend-controller {**all** | **image** | **led** | **manager** | **poe** | **register** | **thermal**}

no debug platform frontend-controller {**all** | **image** | **led** | **manager** | **poe** | **register** | **thermal**}

This command is supported only on Catalyst 3750G-48TS, 3750G-48PS, 3750G-24TS-1U, and 3750G-24PS switches.

Note **Debug** privileged EXEC commands are helpful in diagnosing and resolving internetworking problems and should be used only under the guidance of Cisco technical support staff.

Syntax Description

all	Display all the debug messages for front-end controller.
image	Display Image Manager debug messages.
led	Display LED debug messages.
manager	Display front-end-controller manager debug messages.
poe	Display Power over Ethernet (PoE) debug messages.
register	Display Register Access debug messages.
thermal	Display thermal debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(20)SE3	This command was introduced.

Usage Guidelines

The **undebug platform frontend-controller** command is the same as the **no debug platform frontend-controller** command.

When you enable debugging, it is enabled only on the stack's active switch. To enable debugging on a stack member, start a session from the stack's active switch by using the **session** *switch-number* privileged EXEC command. Then enter the **debug** command at the command-line prompt of the stack member. You can also use the **remote command** *stack-member-number LINE* privileged EXEC command on the stack's active switch to enable debugging on a member switch without first starting a session.

Related Commands

Command	Description
show platform frontend-controller	Displays counter and status information for the front-end controller manager and subordinate applications and displays the hardware and software information for the front-end controller.
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2 > System Management > Troubleshooting and Fault Management**.

show cable-diagnostics tdr

Use the **show cable-diagnostics tdr** privileged EXEC command to display the Time Domain Reflector (TDR) results.

show cable-diagnostics tdr interface *interface-id* [**|** {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	Specify the interface on which TDR was run.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(19)EA1	This command was introduced.

Usage Guidelines

TDR is supported only on copper Ethernet 10/100/1000 ports. It is not supported on 10/100 ports, 10-Gigabit module ports, or small form-factor pluggable (SFP)-module ports. For more information about TDR, see the software configuration guide for this release.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show cable-diagnostics tdr interface** *interface-id* command on a switch other than a Catalyst 3750G-24PS or 3750G-48PS switch:

```
Switch# show cable-diagnostics tdr interface gigabitethernet1/0/2
TDR test last run on: March 01 20:15:40
Interface Speed Local pair Pair length        Remote pair Pair status
--------- ----- ---------- ------------------ ----------- --------------------
Gi1/0/2   auto  Pair A     0    +/- 2  meters N/A         Open

                Pair B     0    +/- 2  meters N/A         Open
                Pair C     0    +/- 2  meters N/A         Open
                Pair D     0    +/- 2  meters N/A         Open
```

This is an example of output from the **show cable-diagnostics tdr interface** *interface-id* command on a Catalyst 3750G-24PS or 3750G-48PS switch:

```
Switch# show cable-diagnostics tdr interface gigabitethernet1/0/2
TDR test last run on: March 01 20:15:40
Interface Speed Local pair Pair length        Remote pair Pair status
--------- ----- ---------- ------------------ ----------- --------------------
Gi1/0/2   auto  Pair A     0    +/- 4 meters  N/A         Open

                Pair B     0    +/- 4 meters  N/A         Open
                Pair C     0    +/- 4 meters  N/A         Open
                Pair D     0    +/- 4 meters  N/A         Open
```

Table 6 lists the descriptions of the fields in the **show cable-diagnostics tdr** command output.

Table 6 Fields Descriptions for the show cable-diagnostics tdr Command Output

Field	Description
Interface	Interface on which TDR was run.
Speed	Speed of connection.
Local pair	Name of the pair of wires that TDR is testing on the local interface.
Pair length	Location on the cable where the problem is, with respect to your switch. TDR can only find the location in one of these cases: • The cable is properly connected, the link is up, and the interface speed is 1000 Mbps. • The cable is open. • The cable has a short.

Table 6 Fields Descriptions for the show cable-diagnostics tdr Command Output (continued)

Field	Description
Remote pair	Name of the pair of wires to which the local pair is connected. TDR can learn about the remote pair only when the cable is properly connected and the link is up.
Pair status	The status of the pair of wires on which TDR is running: • Normal—The pair of wires is properly connected. • Not completed—The test is running and is not completed. • Not supported—The interface does not support TDR. • Open—The pair of wires is open. • Shorted—The pair of wires is shorted.

This is an example of output from the **show interface** *interface-id* command when TDR is running:

```
Switch# show interface gigabitethernet1/0/2
gigabitethernet1/0/2 is up, line protocol is up (connected: TDR in Progress)
```

This is an example of output from the **show cable-diagnostics tdr interface** *interface-id* command when TDR is not running:

```
Switch# show cable-diagnostics tdr interface gigabitethernet1/0/2
% TDR test was never issued on Gi1/0/2
```

If an interface does not support TDR, this message appears:

```
Switch# show cable-diagnostics tdr interface gigabitethernet1/0/28
% TDR test is not supported on switch 1
```

Related Commands

Command	Description
test cable-diagnostics tdr	Enables and runs TDR on an interface.

show controllers power inline

Use the **show controllers power inline** user EXEC command to display the values in the registers of the specified Power over Ethernet (PoE) controller.

show controllers power inline [*instance*] [**module** *switch-number*] [**|** {**begin** **|** **exclude** **|** **include**} *expression*]

Syntax Description

instance	(Optional) Power controller instance, where each instance corresponds to four ports. See the “Usage Guidelines” section for more information. If no instance is specified, information for all instances appear.
module *switch number*	(Optional) Limit the display to ports on the specified stack member. The switch number is 1 to 9.
| begin	(Optional) Display begins with the line that matches the *expression*.

| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(19)EA1	This command was introduced.

Usage Guidelines

For the Catalyst 3750-48PS and 3750G-48PS switches, the *instance* range is 0 to 11.

For the Catalyst 3750-24PS and 3750G-24PS switches, the *instance* range is 0 to 5.

Though visible on all switches, this command is valid only for PoE switches. It provides no information for switches that do not support PoE.

The output provides information that might be useful for Cisco technical support representatives troubleshooting the switch.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show controllers power inline** command on a Catalyst 3750-48PS switch:

```
Switch> show controllers power inline
Module 1, Controller Instance 0, Address 0x40
  Interrupt           Reg 0x0  = 0x0
  Intr Mask           Reg 0x1  = 0xF6
  Power Event         Reg 0x2  = 0x0
  Detect Event        Reg 0x4  = 0x0
  Fault Event         Reg 0x6  = 0x0
  T-Start Event       Reg 0x8  = 0x0
  Supply Event        Reg 0xA  = 0x0
  Port 1 Status       Reg 0xC  = 0x24
  Port 2 Status       Reg 0xD  = 0x24
  Port 3 Status       Reg 0xE  = 0x3
  Port 4 Status       Reg 0xF  = 0x3
  Power Status        Reg 0x10 = 0xFF
  Pin Status          Reg 0x11 = 0x0
  Operating Mode      Reg 0x12 = 0xAA
  Disconnect Enable   Reg 0x13 = 0xA0
  Detect/Class Enable Reg 0x14 = 0xFF
  Reserved            Reg 0x15 = 0x0
  Timing Config       Reg 0x16 = 0x2
  Misc Config         Reg 0x17 = 0xA0
  ID Revision         Reg 0x1A = 0x64

Module 1, Controller Instance 1, Address 0x42
<output truncated>
```

This is an example of output from the **show controllers power inline** command on a Catalyst 3750G-48PS switch:

```
Switch> show controllers power inline
Alchemy instance 0, address 0

Alchemy instance 1, address 7

Alchemy instance 2, address E
```

Related Commands

Command	Description
logging event power-inline-status	Enables the logging of PoE events.
powerinline	Configures the power management mode for the specified PoE port or for all PoE ports.
show power inline	Displays the PoE status for the specified PoE port or for all PoE ports.

show env

Use the **show env** user EXEC command to display fan, temperature, redundant power system (RPS) availability, and power information for the switch being accessed (standalone switch, active switch, or member switches). Use with the **stack** keyword to display all information for the stack or for a specified switch in the stack.

show env {**all** | **fan** | **power** | **rps** | **stack** [*switch-number*] | **temperature [status]**} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

all	Display both fan and temperature environmental status.
fan	Display the switch fan status.
power	Display the switch power status.
rps	Display whether an RPS 300 Redundant Power System is connected to the switch.
stack [*switch-number*]	Display all environmental status for each switch in the stack or for the specified switch. The range is 1 to 9, depending on the switch member numbers in the stack.
temperature	Display the switch temperature status.
status	(Optional) Display the switch internal temperature (not the external temperature) and the threshold values. This keyword is available only on the Catalyst 3750G-48TS, 3750G-48PS, 3750G-24TS-1U, and 3750G-24PS switches.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was introduced.
12.2(20)SE3	The **temperature status** keyword was added.

Usage Guidelines

Use the **show access-lists** privileged EXEC command to access information from a specific switch other than the active switch.

You can use the **show env stack** [*switch-number*] command to display information about any switch in the stack from any member switch.

Though visible on all switches, the **show env temperature status** command is valid only for the Catalyst 3750G-48TS, 3750G-48PS, 3750G-24TS-1U, and 3750G-24PS switches. If you enter this command on these switches, the command output shows the switch temperature states and the threshold levels. The switch temperature is the temperature in the switch, not the external temperature. If you enter the command on a switch other than those four, the output field shows `Not Applicable`.

On a Catalyst 3750G-48PS or 3750G-24PS switch, you can also use the **show env temperature** command to display the switch temperature status. The command output shows the green and yellow states as *OK* and the red state as *FAULTY*. If you enter the **show env all** command on this switch, the command output is the same as the **show env temperature status** command output.

For more information about the threshold levels, see the software configuration guide for this release.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show env all** command entered from the active switch or a standalone switch:

```
Switch> show env all
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is AVAILABLE
```

This is an example of output from the **show env fan** command:

```
Switch> show env fan
FAN is OK
```

This is an example of output from the **show env stack** command:

```
Switch> show env stack
SWITCH: 1
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
SWITCH: 2
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
SWITCH: 3
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
```

```
SWITCH: 4
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
SWITCH: 5
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
SWITCH: 6
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
```

This example shows how to display information about stack member 3 from the active switch:

```
Switch> show env stack 3
SWITCH: 3
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
```

This example shows how to display the temperature value, state, and the threshold values. Table 7 describes the temperature states in the command output.

```
Switch> show env temperature status
Temperature Value:28 Degree Celsius
Temperature State:GREEN
Yellow Threshold :70 Degree Celsius
Red Threshold    :75 Degree Celsius
```

Table 7 States in the show env temperature status Command Output

State	Description
Green	The switch temperature is in the *normal* operating range.
Yellow	The temperature is in the *warning* range. You should check the external temperature around the switch.
Red	The temperature is in the *critical* range. The switch might not run properly if the temperature is in this range.

system env temperature threshold yellow

Use the **system env temperature threshold yellow** global configuration command on the switch stack or on a standalone switch to specify the difference between the yellow and red temperature thresholds and to configure the yellow threshold. Use the **no** form of this command to return to the default value.

system env temperature threshold yellow *value*

no system env temperature threshold yellow *value*

Syntax Description

value	Specify the difference between the yellow and red threshold values (in Celsius). The range is 10 to 25. The default value is 10.

Defaults

These are the default values:

Table 8 Default Values for the Temperature Thresholds

Switch	Yellow	Red[1]
Catalyst 3750G-48TS	10°C	66°C
Catalyst 3750G-48PS	10°C	68°C
Catalyst 3750G-24TS-1U	10°C	65°C
Catalyst 3750G-24PS	10°C	61°C

1. You cannot configure the red temperature threshold.

Command Modes

Global configuration

Command History

Release	Modification
12.2(20)SE3	This command was introduced.

Usage Guidelines

Though visible on all switches, this command is only valid on these switches:

- Catalyst 3750G-48TS
- Catalyst 3750G-48PS
- Catalyst 3750G-24TS-1U
- Catalyst 3750G-24PS

You cannot configure the green and red thresholds but can configure the yellow threshold. Use the **system env temperature threshold yellow** *value* global configuration command to specify the difference between the yellow and red thresholds and to configure the yellow threshold. For example, if the red threshold is 66 degrees C and you want to configure the yellow threshold as 51 degrees C, set the difference between the thresholds as 15 by using the **system env temperature threshold yellow 15** command.

Note The internal temperature sensor in the switch measures the internal system temperature and might vary ±5 degrees C.

Examples

This example sets 5 as the difference between the yellow and red thresholds:

```
Switch(config)# system env temperature threshold yellow 15
Switch(config)#
```

Related Commands

Command	Description
show env temperature status	Displays the temperature status and threshold levels.

show platform frontend-controller

Use the **show platform frontend-controller** privileged EXEC command to display counter and status information for the front-end controller manager and subordinate applications and to display the hardware and software information for the front-end controller.

show platform frontend-controller {**buffer** | **generic** | **manager** *number* | **subordinate** *number* | **version** *number*} [| {**begin** | **exclude** | **include**} *expression*]

This command is supported only on Catalyst 3750G-48TS, 3750G-48PS, 3750G-24TS-1U, and 3750G-24PS switches.

Note **Show platform** privileged EXEC commands display information helpful in diagnosing and resolving internetworking problems and should be used only under the guidance of Cisco technical support staff.

Syntax Description

buffer	Display the last 1024 bytes sent from the manager to the subordinate and the reverse.
generic	Display the generic counters that do not specifically apply to the manager or subordinate.
manager *number*	Display the counters for the manager and the subordinate specified by *number*. See the "Usage Guidelines" section for the *number* range.
subordinate *number*	Display the subordinate status and the counters for the subordinate specified by *number*. See the "Usage Guidelines" section for the *number* range.
version *number*	Display the hardware and software version information for the subordinate status specified by *number*. See the "Usage Guidelines" section for the *number* range.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(20)SE3	This command was introduced.

Usage Guidelines

On the Catalyst 3750G-48TS and 3750G-48PS switches, the subordinate number range is 0 to 2.

On the Catalyst 3750G-24TS-1U and 3750G-24PS switches, the subordinate number range is 0 to 1.

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Documentation Updates for Catalyst 3560 Switches Running Cisco IOS Release 12.2(20)SE3

The following commands are supported on the Catalyst 3560G-24PS, 3560G-24TS, 3560G-48PS, and 3560G-48TS switches and will be included in the next version of the Catalyst 3560 command reference.

The **test cable-diagnostics tdr** privileged EXEC command is also supported on the Catalyst 3560G-24PS, 3560G-24TS, 3560G-48PS, and 3560G-48TS switches beginning with Cisco IOS Release 12.2(20)SE3.

debug platform frontend-controller

Use the **debug platform frontend-controller** privileged EXEC command to enable debugging of front-end controller activity. Use the **no** form of this command to disable debugging.

debug platform frontend-controller {**all** | **image** | **led** | **manager** | **poe** | **register** | **thermal**}

no debug platform frontend-controller {**all** | **image** | **led** | **manager** | **poe** | **register** | **thermal**}

This command is supported only on Catalyst 3560G-48TS, 3560G-48PS, 3560G-24TS, and 3560G-24PS switches.

Note **Debug** privileged EXEC commands are helpful in diagnosing and resolving internetworking problems and should be used only under the guidance of Cisco technical support staff.

Syntax Description

all	Display all the debug messages for front-end controller.
image	Display Image Manager debug messages.
led	Display LED debug messages.
manager	Display front-end-controller manager debug messages.
poe	Display Power over Ethernet (PoE) debug messages.
register	Display Register Access debug messages.
thermal	Display thermal debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(20)SE3	This command was introduced.

Usage Guidelines

The **undebug platform frontend-controller** command is the same as the **no debug platform frontend-controller** command.

Related Commands

Command	Description
show platform frontend-controller	Displays counter and status information for the front-end controller manager and subordinate applications and displays the hardware and software information for the front-end controller.
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2 > System Management > Troubleshooting and Fault Management**.

show cable-diagnostics tdr

Use the **show cable-diagnostics tdr** privileged EXEC command to display the Time Domain Reflector (TDR) results.

show cable-diagnostics tdr interface *interface-id* [**|** {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	Specify the interface on which TDR was run.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(20)SE3	This command was introduced.

Usage Guidelines

TDR is supported only on copper Ethernet 10/100/1000 ports. It is not supported on 10/100 ports, 10-Gigabit module ports, or small form-factor pluggable (SFP)-module ports. For more information about TDR, see the software configuration guide for this release.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show cable-diagnostics tdr interface** *interface-id* command on a switch other than a Catalyst 3560G-24PS or 3560G-48PS switch:

```
Switch# show cable-diagnostics tdr interface gigabitethernet0/2
TDR test last run on: March 01 20:15:40
Interface Speed Local pair Pair length        Remote pair Pair status
--------- ----- ---------- ------------------ ----------- --------------------
Gi0/2     auto  Pair A     0    +/- 2  meters N/A         Open

                Pair B     0    +/- 2  meters N/A         Open
                Pair C     0    +/- 2  meters N/A         Open
                Pair D     0    +/- 2  meters N/A         Open
```

This is an example of output from the **show cable-diagnostics tdr interface** *interface-id* command on a Catalyst 3560G-24PS or 3560G-48PS switch:

```
Switch# show cable-diagnostics tdr interface gigabitethernet0/2
TDR test last run on: March 01 20:15:40
Interface Speed Local pair Pair length        Remote pair Pair status
--------- ----- ---------- ------------------ ----------- --------------------
Gi0/2     auto  Pair A     0    +/- 4 meters  N/A         Open

                Pair B     0    +/- 4 meters  N/A         Open
                Pair C     0    +/- 4 meters  N/A         Open
                Pair D     0    +/- 4 meters  N/A         Open
```

Table 9 lists the descriptions of the fields in the **show cable-diagnostics tdr** command output.

Table 9 Fields Descriptions for the show cable-diagnostics tdr Command Output

Field	Description
Interface	Interface on which TDR was run.
Speed	Speed of connection.
Local pair	Name of the pair of wires that TDR is testing on the local interface.
Pair length	Location on the cable where the problem is, with respect to your switch. TDR can only find the location in one of these cases: • The cable is properly connected, the link is up, and the interface speed is 1000 Mbps. • The cable is open. • The cable has a short.
Remote pair	Name of the pair of wires to which the local pair is connected. TDR can learn about the remote pair only when the cable is properly connected and the link is up.
Pair status	The status of the pair of wires on which TDR is running: • Normal—The pair of wires is properly connected. • Not completed—The test is running and is not completed. • Not supported—The interface does not support TDR. • Open—The pair of wires is open. • Shorted—The pair of wires is shorted.

This is an example of output from the **show interface** *interface-id* command when TDR is running:

```
Switch# show interface gigabitethernet0/2
gigabitethernet0/2 is up, line protocol is up (connected: TDR in Progress)
```

This is an example of output from the **show cable-diagnostics tdr interface** *interface-id* command when TDR is not running:

```
Switch# show cable-diagnostics tdr interface gigabitethernet0/2
% TDR test was never issued on Gi0/2
```

If an interface does not support TDR, this message appears:

```
Switch# show cable-diagnostics tdr interface gigabitethernet0/28
% TDR test is not supported on switch 1
```

Related Commands

Command	Description
test cable-diagnostics tdr	Enables and runs TDR on an interface.

show controllers power inline

Use the **show controllers power inline** user EXEC command to display the values in the registers of the specified Power over Ethernet (PoE) controller.

show controllers power inline [*instance*] [**|** {**begin** | **exclude** | **include**} *expression*]

Syntax Description

instance	(Optional) Power controller instance, where each instance corresponds to four ports. See the "Usage Guidelines" section for more information. If no instance is specified, information for all instances appear.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(19)EA1	This command was introduced.

Usage Guidelines

For the Catalyst 3560-48PS and 3560G-48PS switches, the *instance* range is 0 to 11.

For the Catalyst 3560-24PS and 3560G-24PS switches, the *instance* range is 0 to 5.

Though visible on all switches, this command is valid only for PoE switches. It provides no information for switches that do not support PoE.

The output provides information that might be useful for Cisco technical support representatives troubleshooting the switch.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show controllers power inline** command on a Catalyst 3560-48PS switch:

```
Switch> show controllers power inline
Controller Instance 0, Address 0x40
Interrupt           Reg 0x0  = 0x0
Intr Mask           Reg 0x1  = 0xF6
Power Event         Reg 0x2  = 0x0
Detect Event        Reg 0x4  = 0x0
Fault Event         Reg 0x6  = 0x0
T-Start Event       Reg 0x8  = 0x0
Supply Event        Reg 0xA  = 0x0
Port 1 Status       Reg 0xC  = 0x64
Port 2 Status       Reg 0xD  = 0x3
Port 3 Status       Reg 0xE  = 0x3
Port 4 Status       Reg 0xF  = 0x3
Power Status        Reg 0x10 = 0xFF
Pin Status          Reg 0x11 = 0x0
Operating Mode      Reg 0x12 = 0xAA
Disconnect Enable   Reg 0x13 = 0xF0
Detect/Class Enable Reg 0x14 = 0xFF
Reserved            Reg 0x15 = 0x0
Timing Config       Reg 0x16 = 0x0
Misc Config         Reg 0x17 = 0xA0
ID Revision         Reg 0x1A = 0x64

Controller Instance 1, Address 0x42
<output truncated>
```

This is an example of output from the **show controllers power inline** command on a Catalyst 3560G-48PS switch:

```
Switch> show controllers power inline
Alchemy instance 0, address 0

Alchemy instance 1, address 7

Alchemy instance 2, address E
```

Related Commands

Command	Description
logging event power-inline-status	Enables the logging of PoE events.
power inline	Configures the power management mode for the specified PoE port or for all PoE ports.
show power inline	Displays the PoE status for the specified PoE port or for all PoE ports.

show env

Use the **show env** user EXEC command to display fan, temperature, redundant power system (RPS) availability, and power information for the switch.

show env {**all** | **fan** | **power** | **rps**| **temperature [status]**} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

all	Display both fan and temperature environmental status.
fan	Display the switch fan status.
power	Display the switch power status.
rps	Display whether an RPS 300 Redundant Power System is connected to the switch.
temperature	Display the switch temperature status.
status	(Optional) Display the switch internal temperature (not the external temperature) and the threshold values. This keyword is available only on the Catalyst 3560G-48TS, 3560G-48PS, 3560G-24TS, and 3560G-24PS switches.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(19)EA1	This command was introduced.
12.2(20)SE3	The **temperature status** keyword was added.

Usage Guidelines

Though visible on all switches, the **show env temperature status** command is valid only for the Catalyst 3560G-48TS, 3560G-48PS, 3560G-24TS, and 3560G-24PS switches. If you enter this command on these switches, the command output shows the switch temperature states and the threshold levels. The switch temperature is the temperature in the switch, not the external temperature. If you enter the command on a switch other than those four, the output field shows `Not Applicable`.

On a Catalyst 3560G-48PS or 3560G-24PS switch, you can also use the **show env temperature** command to display the switch temperature status. The command output shows the green and yellow states as *OK* and the red state as *FAULTY*. If you enter the **show env all** command on this switch, the command output is the same as the **show env temperature status** command output.

For more information about the threshold levels, see the software configuration guide for this release.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show env all** command entered:

```
Switch> show env all
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is AVAILABLE
```

This is an example of output from the **show env fan** command:

```
Switch> show env fan
FAN is OK
```

This example shows how to display the temperature value, state, and the threshold values. Table 10 describes the temperature states in the command output.

```
Switch> show env temperature status
Temperature Value:28 Degree Celsius
Temperature State:GREEN
Yellow Threshold :70 Degree Celsius
Red Threshold    :75 Degree Celsius
```

Table 10 States in the show env temperature status Command Output

State	Description
Green	The switch temperature is in the *normal* operating range.
Yellow	The temperature is in the *warning* range. You should check the external temperature around the switch.
Red	The temperature is in the *critical* range. The switch might not run properly if the temperature is in this range.

system env temperature threshold yellow

Use the **system env temperature threshold yellow** global configuration command to specify the difference between the yellow and red temperature thresholds and to configure the yellow threshold. Use the **no** form of this command to return to the default value.

system env temperature threshold yellow *value*

no system env temperature threshold yellow *value*

Syntax Description

value	Specify the difference between the yellow and red threshold values (in Celsius). The range is 10 to 25. The default value is 10.

Defaults

These are the default values:

Table 11 Default Values for the Temperature Thresholds

Switch	Yellow	Red[1]
Catalyst 3560G-48TS	10°C	66°C
Catalyst 3560G-48PS	10°C	68°C
Catalyst 3560G-24TS	10°C	65°C
Catalyst 3560G-24PS	10°C	61°C

1. You cannot configure the red temperature threshold.

Command Modes

Global configuration

Command History

Release	Modification
12.2(20)SE3	This command was introduced.

Usage Guidelines

Though visible on all switches, this command is only valid on these switches:

- Catalyst 3560G-48TS
- Catalyst 3560G-48PS
- Catalyst 3560G-24TS
- Catalyst 3560G-24PS

You cannot configure the green and red thresholds but can configure the yellow threshold. Use the **system env temperature threshold yellow** *value* global configuration command to specify the difference between the yellow and red thresholds and to configure the yellow threshold. For example, if the red threshold is 66 degrees C and you want to configure the yellow threshold as 51 degrees C, set the difference between the thresholds as 15 by using the **system env temperature threshold yellow 15** command.

Note The internal temperature sensor in the switch measures the internal system temperature and might vary ±5 degrees C.

Examples

This example sets 5 as the difference between the yellow and red thresholds:

```
Switch(config)# system env temperature threshold yellow 15
Switch(config)#
```

Related Commands

Command	Description
show env temperature status	Displays the temperature status and threshold levels.

show platform frontend-controller

Use the **show platform frontend-controller** privileged EXEC command to display counter and status information for the front-end controller manager and subordinate applications and to display the hardware and software information for the front-end controller.

show platform frontend-controller {**buffer** | **generic** | **manager** *number* | **subordinate** *number* | **version** *number*} [| {**begin** | **exclude** | **include**} *expression*]

This command is supported only on Catalyst 3560G-48TS, 3560G-48PS, 3560G-24TS, and 3560G-24PS switches.

Note **Show platform** privileged EXEC commands display information helpful in diagnosing and resolving internetworking problems and should be used only under the guidance of Cisco technical support staff.

Syntax Description

buffer	Display the last 1024 bytes sent from the manager to the subordinate and the reverse.
generic	Display the generic counters that do not specifically apply to the manager or subordinate.
manager *number*	Display the counters for the manager and the subordinate specified by *number*. See the "Usage Guidelines" section for the *number* range.
subordinate *number*	Display the subordinate status and the counters for the subordinate specified by *number*. See the "Usage Guidelines" section for the *number* range.
version *number*	Display the hardware and software version information for the subordinate status specified by *number*. See the "Usage Guidelines" section for the *number* range.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(20)SE3	This command was introduced.

Usage Guidelines

On the Catalyst 3560G-48TS and 3560G-48PS switches, the subordinate number range is 0 to 2.

On the Catalyst 3560G-24TS and 3560G-24PS switches, the subordinate number range is 0 to 1.

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Documentation Updates for Cisco IOS Release 12.2(20)SE1

These updates were added for Cisco IOS Release 12.2(20)SE1:

- "Addition to the Catalyst 3750 and 3560 Switch Software Configuration Guides" section on page 54
- "Revisions to the Catalyst 3750, 3560, and 2970 Switch Command References" section on page 54
- "Revisions to the Catalyst 3750 and 3560 System Message Guides" section on page 55
- "Addition to the Catalyst 3750 Switch System Message Guide" section on page 57
- "Additions to the Catalyst 3560 Switch System Message Guide" section on page 57

Addition to the Catalyst 3750 and 3560 Switch Software Configuration Guides

This section was added to the "Troubleshooting Power over Switch Ethernet Switch Ports" section of the Catalyst 3750 and 3560 "Troubleshooting" chapters.

Disabled Port Caused by False Link Up

If a Power over Ethernet (PoE) switch powered device, such as a Cisco IP Phone, is connected to a port and you configure the port by using the **power inline never** interface configuration command, a false link up can place the port into an error-disabled state. To take the port out of the error-disabled state, enter the **shutdown** and **no shutdown** interface configuration commands.

You should not connect a PoE-powered device to a port on a PoE switch if that port has been configured with the **power inline never** command.

Revisions to the Catalyst 3750, 3560, and 2970 Switch Command References

These commands were revised for the Catalyst 3750, 3560, and 2970 switch command references:

- You can now configure the **duplex** setting when the speed is set to **auto**. In previous releases, you could not configure the duplex setting when an interface was configured to autonegotiate.
- You can now specify the **speed** at which a port autonegotiates.

  This example shows how to set a port to autonegotiate at only 10 Mbps:

  ```
  Switch(config)# interface fastethernet0/1
  Switch(config-if)# speed auto 10
  ```

  This example shows how to set a port to autonegotiate at only 10 or 100 Mbps:

  ```
  Switch(config)# interface fastethernet0/1
  Switch(config-if)# speed auto 10 100
  ```

- When you configure a port by using the **power inline auto** interface configuration command, the port autonegotiates by using the configured speed and duplex settings. This is necessary to determine the power requirements of the connected device (whether or not it is a powered device). After the power requirements have been determined, the switch hardcodes the interface by using the configured speed and duplex settings without resetting the interface.
- When you configure a port by using the **power inline never** command, the port reverts to the configured speed and duplex settings.

  If a port has a device that is powered by a PoE switch connected to it, you should not use the **power inline never** command to configure the port. A false link up can occur on the port and place it into an error-disabled state.

  In releases earlier than Cisco IOS Release 12.2(20)SE1, power was sometimes still applied to a PoE switch port even after a PoE-powered device was removed. This could cause damage to a non-PoE-powered device when it was later connected to that port. Make sure that your switch is running Cisco IOS Release 12.2(20)SE1 or later.
- You can use the **show interfaces transceiver properties** privileged EXEC command to show the speed, duplex, and inline power status PoE switches for an interface.

  This is an example of output from the **show interfaces transceiver properties** command. If you do not specify an interface, the output of the command shows the status on all switch ports:

  ```
  Switch# show interfaces transceiver properties
  Name : Fa1/0/1
  Administrative Speed: auto
  ```

```
Operational Speed: auto
Administrative Duplex: auto
Administrative Power Inline: enable
Operational Duplex: auto
Administrative Auto-MDIX: off
Operational Auto-MDIX: off

Name : Fa1/0/2
Administrative Speed: auto
Operational Speed: auto
Administrative Duplex: auto
Administrative Power Inline: enable
Operational Duplex: auto
Administrative Auto-MDIX: off
Operational Auto-MDIX: off

<output truncated>
```

This is an example of output from the **show interfaces module** *number* **transceiver properties** command for a specific interface:

```
Switch# show interfaces fastethernet0/1 transceiver properties
Name : Fa1/0/1
Administrative Speed: auto
Administrative Duplex: auto
Administrative Auto-MDIX: on
Administrative Power Inline: enable
Operational Speed: auto
Operational Duplex: auto
Operational Auto-MDIX: on
```

Revisions to the Catalyst 3750 and 3560 System Message Guides

These messages have been revised in the "Catalyst 3750 Switch System Message Guide" and the "Catalyst 3560 Switch System Message Guide."

Error Message `ETHCNTR-3-HALF_DUX_COLLISION_EXCEED_THRESHOLD: Collision at [chars] exceed threshold. Consider as loop-back.`

Explanation This message means that the collisions at a half-duplex port exceeded the threshold, and the port is considered as a loopback. On switches that support Power over Ethernet (PoE), this message might be displayed when a device that can be powered by either a PoE switch port or by AC power is not being powered by an external AC power source and is connected to a port that has been configured with the **power inline never** interface configuration command. [chars] is the port where the threshold was exceeded.

Recommended Action On switches that support PoE, remove the device or configure the port by entering the **power inline auto**, **shutdown**, and **no shutdown** interface configuration commands. No action is required on non-PoE switches. The port goes into error-disabled mode until the problem is resolved.

Error Message `ETHCNTR-3-LOOP_BACK_DETECTED: Loop-back detected on [chars].`

Explanation This message means that a loopback condition might be the result of a balun cable incorrectly connected into a port. On PoE switches, this message might be displayed when device that can be powered by either a PoE switch port or by AC power is not being powered by an external AC power source and is connected to a port that has been configured with the **power inline never** interface configuration command. [chars] is the interface name.

Recommended Action On non-PoE switches, check the cables. If a balun cable is connected and the loopback condition is desired, no action is required. Otherwise, connect the correct cable, and then enable the port. On PoE switches, remove the device or configure the port by entering the **power inline auto**, **shutdown**, **and no shutdown** interface configuration commands.

Error Message `PM-4-ERR_DISABLE: [chars] error detected on [chars], putting [chars] in err-disable state.`

Explanation This message means that the port manager detected a misconfiguration or misbehavior and placed the interface in an error-disabled state. A recovery is attempted after the configured retry time (the default is 5 minutes). On PoE switches, this message might appear when a device that can be powered by either a PoE switch port or by AC power is not being powered by an external AC power source and is connected to a port that has been configured with the **power inline never** interface configuration command. [chars] is the port where the threshold was exceeded. The first [chars] is the error, and the second and third [chars] are the affected interfaces.

Recommended Action On non-PoE switches, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Enter the **show tech-support** user EXEC command to gather data that might help identify the nature of the error. Use the Bug Toolkit to look for similar reported problems. On PoE switches, remove the device or configure the port by entering the **power inline auto**, **shutdown**, and **no shutdown** interface configuration commands. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the see the "Error Message Traceback Reports" section.

Error Message `ILPOWER-5-IEEE-DISCONNECT: Interface [chars]: PD removed.`

Explanation This message means that the powered device is no longer connected to the switch or that the connected powered device is being powered by an external AC power source. The switch is no longer providing power to the port. [chars] is the interface.

Recommended Action No action is required.

Addition to the Catalyst 3750 Switch System Message Guide

This is a new message for the "Catalyst 3750 Switch System Message Guide."

BADTRANSCEIVER Messages

This section contains the BADTRANSCEIVER message.

Error Message `BADTRANSCEIVER, PHY, LOG_WARNING: An inappropriate transceiver has been inserted in interface [chars].`

Explanation This message means that a defective module is installed in the specified interface. [chars] is the interface.

Recommended Action Remove the transceiver. If it was purchased from Cisco, contact your Cisco representative to have the transceiver replaced.

Additions to the Catalyst 3560 Switch System Message Guide

These are new messages for the "Catalyst 3560 Switch System Message Guide".

Error Message `ILPOWER-3-CONTROLLER_ERR: Controller error, Controller number [dec]: [chars].`

Explanation This message means that an error reported or caused by the PoE controller is detected. [dec] is the controller instance, which is 0 to 5 on a 24-port PoE switch and 0 to 11 on a 48-port PoE switch. [chars] describes the error.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Enter the **show tech-support** user EXEC command to gather data that might help identify the nature of the error. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the see the "Error Message Traceback Reports" section.

Error Message `ILPOWER-3-CONTROLLER_IF_ERR: Controller interface error, [chars] [chars].`

Explanation This message means that an interface error is detected between the PoE controller and the system. The first [chars] is the interface. The second [chars] describes the error.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Enter the **show tech-support** user EXEC command to gather data that might help identify the nature of the error. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the see the "Error Message Traceback Reports" section.

Error Message `ILPOWER-3-CONTROLLER_PORT_ERR: Controller port error, Interface [chars]: [chars]`

Explanation This message means that a port error reported by the PoE controller is detected. The first [chars] is the interface. The second [chars] describes the error.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Enter the **show tech-support** user EXEC command to gather data that might help identify the nature of the error. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the "Error Message Traceback Reports" section.

Error Message `ILPOWER-3-ILPOWER_INTERNAL_IF_ERROR: Inline Power internal error, interface [chars]: [chars].`

Explanation This message means that a software check failed during PoE processing. The first [chars] is the interface. The second [chars] describes the error.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Enter the **show tech-support** user EXEC command to gather data that might help identify the nature of the error. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the "Error Message Traceback Reports" section.

Error Message `ILPOWER-5-IEEE_DISCONNECT: Interface [chars]: AC disconnect`

Explanation This message means that the powered device is no longer connected to the switch or that the connected powered device is being powered by an external AC power source. No power is on the switch PoE port. [chars] is the interface.

Recommended Action No action is required.

Error Message `ILPOWER-5-ILPOWER_POWER_DENY: Interface [chars]: inline power denied.`

Explanation This message means that there is not enough power remaining in the switch to supply to the PoE port. [chars] is the interface.

Recommended Action Connect the powered device to an external AC power source.

Error Message `ILPOWER-5-POWER_GRANTED: Interface [chars]: Power granted.`

Explanation This message means that there is enough power available in the switch and that power is on the PoE port. [chars] is the interface.

Recommended Action No action is required.

Error Message `ILPOWER-7-DETECT: Interface [chars]: Power Device detected:[chars].`

Explanation This message means that the switch has detected the attached powered device. The first [chars] is the interface. The second [chars] is the Cisco pre-standard powered device or the IEEE-compliant powered device.

Recommended Action No action is required.

Documentation Updates for Cisco IOS Release 12.2(20)SE

These updates were added for Cisco IOS Release 12.2(20)SE1:

- "Corrections to the Catalyst 3750, 3560, and 2970 Switch Software Configuration Guides" section on page 59
- "Additions to the Catalyst 3750 Switch Software Configuration Guide" section on page 59
- "Additions to the Catalyst 3750 Switch Command Reference" section on page 63

Corrections to the Catalyst 3750, 3560, and 2970 Switch Software Configuration Guides

In printed copies of the software configuration guides, the URL listed in the "Privilege Levels" section of the "Getting Started with CMS" chapter is incorrect. The section lists this URL:

http://ip_address/level/13

This is the correct URL (the closing "/" is required):

http://ip_address/level/13/

In printed copies of the software configuration guides, in the "Classifying Traffic by Using ACLs" section of the "Configuring QoS" chapter, this information in Step 3 to create a Layer 2 MAC ACL is incorrect:

- For *src-MAC-addr*, enter the MAC address of the host from which the packet is being sent. You specify this by using the hexadecimal format (H.H.H), by using the **any** keyword as an abbreviation for *source* 0.0.0, *source-wildcard* 255.255.255, or by using the **host** keyword for *source* 0.0.0.
- For *dst-MAC-addr*, enter the MAC address of the host to which the packet is being sent. You specify this by using the hexadecimal format (H.H.H), by using the **any** keyword as an abbreviation for *source* 0.0.0, *source-wildcard* 255.255.255, or by using the **host** keyword for *source* 0.0.0.

This is the correct information:

- For *src-MAC-addr*, enter the MAC address of the host from which the packet is being sent. You specify this by using the hexadecimal format (H.H.H), by using the **any** keyword as an abbreviation for *source* 0.0.0, *source-wildcard* ffff.ffff.ffff, or by using the **host** keyword for *source* 0.0.0.
- For *dst-MAC-addr*, enter the MAC address of the host to which the packet is being sent. You specify this by using the hexadecimal format (H.H.H), by using the **any** keyword as an abbreviation for *source* 0.0.0, *source-wildcard* ffff.ffff.ffff, or by using the **host** keyword for *source* 0.0.0.

Additions to the Catalyst 3750 Switch Software Configuration Guide

The next sections provide updated information for the "Managing Switch Stacks" chapter.

Major Version Number Incompatibility Among Switches

Note The information in the "Major Incompatibility Between Switches" section was retitled and should be replaced with this information.

Switches with different Cisco IOS software versions likely have different stack protocol versions. Switches with different major version numbers are incompatible and cannot exist in the same switch stack.

Minor Version Number Incompatibility Among Switches

Note The information in the "Minor Incompatibility Between Switches" section was retitled and should be replaced with this information.

Switches with the same major version number but with a different minor version number as the stack's active switch are considered partially compatible. When connected to a switch stack, a partially compatible switch enters version-mismatch (VM) mode and cannot join the stack as a fully functioning member. The software detects the mismatched software and tries to upgrade (or downgrade) the switch in VM mode with the switch stack image or with a tar file image from the switch stack flash memory. The software uses the automatic upgrade (auto-upgrade) and the automatic advise (auto-advise) features. For more information, see the "Understanding Auto-Upgrade and Auto-Advise" section on page 60.

To see if there are switches in VM mode, use the **show switch** user EXEC command. The port LEDs on switches in VM mode will also stay off. Pressing the Mode button does not change the LED mode.

Understanding Auto-Upgrade and Auto-Advise

Note This is a new section, not previously in the "Managing Switch Stacks" chapter.

When the software detects mismatched software and tries to upgrade the switch in VM mode, two software processes are involved:

- Automatic upgrade (auto-upgrade)—a process that automatically copies (auto-copy) the software image running on any stack member or copies a tar file from the switch stack flash memory to the switch in VM mode to upgrade (auto-upgrade) it. By default, auto-upgrade is enabled (the **boot auto-copy-sw** global configuration command is enabled). You can disable auto-upgrade by using the **no boot auto-copy-sw** global configuration command on the stack's active switch. You can check the status of auto-upgrade by using the **show boot** privileged EXEC command and by checking the *Auto upgrade* line in the display.

  Auto-upgrade occurs if it is enabled, if there is enough flash memory in the switch in VM mode, and if:

  - The software image running on the switch stack is suitable for the switch in VM mode, or
  - There is a tar file from the switch stack that is suitable for the switch in VM mode. A switch in VM mode might not run all released software. For example, new switch hardware is not recognized in earlier versions of software.

  The auto-upgrade and the auto-copy processes wait for a few minutes before starting.

When the auto-upgrade process is complete, the switch that was in VM mode reloads and joins the stack as a fully functioning member. If you have both StackWise cables connected during the reload, network downtime does not occur because the switch stack operates on two rings.

Note Auto-upgrade performs the upgrade only when the two images are the same type. For example, it does not automatically upgrade a switch in VM mode from EMI to SMI (or the reverse) or from cryptographic to noncryptographic (or the reverse).

- Automatic advise (auto-advise)—when the auto-upgrade process cannot find appropriate stack member software to copy to the switch in VM mode, the auto-advise process tells you the command (**archive copy-sw** or **archive download-sw** privileged EXEC command) and the image name (tar filename) needed to manually upgrade the switch stack or the switch in VM mode. The recommended image can be the running switch stack image or a tar file in any flash file system in the switch stack (including the switch in VM mode). Auto-advise cannot be disabled, and there is no command to check its status.

  The auto-advise software does *not* give suggestions when the switch stack software and the software of the switch in VM mode do not contain the same feature sets. For example, if the switch stack is running the SMI and you add a switch that is running the EMI, the auto-advise software does not provide a recommendation. The same events occur when cryptographic and noncryptographic images are running.

Auto-Upgrade and Auto-Advise Example Messages

Note This is a new section, not previously in the “Managing Switch Stacks” chapter.

When you add a switch that has a different minor version number to the switch stack, the software displays messages in sequence (assuming that there are no other system messages generated by the switch).

This example shows that the switch stack detected a new switch that is running a different minor version number than the switch stack. Auto-copy launches, finds suitable software to copy from a stack member to the switch in VM mode, upgrades the switch in VM mode, and then reloads it:

```
*Mar 11 20:31:19.247:%STACKMGR-6-STACK_LINK_CHANGE:Stack Port 2 Switch 2 has changed to
state UP
*Mar 11 20:31:23.232:%STACKMGR-6-SWITCH_ADDED_VM:Switch 1 has been ADDED to the stack
(VERSION_MISMATCH)
*Mar 11 20:31:23.291:%STACKMGR-6-SWITCH_ADDED_VM:Switch 1 has been ADDED to the stack
(VERSION_MISMATCH) (Stack_1-3)
*Mar 11 20:33:23.248:%IMAGEMGR-6-AUTO_COPY_SW_INITIATED:Auto-copy-software process
initiated for switch number(s) 1
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:Searching for stack member to act
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:as software donor...
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:Found donor (system #2) for
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:member(s) 1
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:System software to be uploaded:
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:System Type:            0x00000000
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:archiving c3750-i5-mz.122-0.0.313.SE
(directory)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:archiving
c3750-i5-mz.122-0.0.313.SE/c3750-i5-mz.122-0.0.313.SE.bin (4945851 bytes)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:archiving c3750-i5-mz.122-0.0.313.SE/info
(450 bytes)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:archiving info (104 bytes)
```

```
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:examining image...
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:extracting info (104 bytes)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:extracting c3750-i5-mz.122-0.0.313.SE/info
(450 bytes)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:extracting info (104 bytes)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:Stacking Version Number:1.4
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:System Type:            0x00000000
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:  Ios Image File Size:  0x004BA200
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:  Total Image File Size:0x00818A00
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:  Minimum Dram required:0x04000000
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:  Image Suffix:i5-122-0.0.313.SE
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:  Image Directory:c3750-i5-mz.122-0.0.313.SE
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:  Image Name:c3750-i5-mz.122-0.0.313.SE.bin
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:  Image Feature:LAYER_3|MIN_DRAM_MEG=64
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:Old image for switch
1:flash1:c3750-i5-mz.121-19.EA1
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:  Old image will be deleted after download.
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:Extracting images from archive into flash on
switch 1...
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:c3750-i5-mz.122-0.0.313.SE (directory)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:extracting
c3750-i5-mz.122-0.0.313.SE/c3750-i5-mz.122-0.0.313.SE.bin (4945851 bytes)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:extracting c3750-i5-mz.122-0.0.313.SE/info
(450 bytes)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:extracting info (104 bytes)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:Installing
(renaming):`flash1:update/c3750-i5-mz.122-0.0.313.SE' ->
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:       `flash1:c3750-i5-mz.122-0.0.313.SE'
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:New software image installed in
flash1:c3750-i5-mz.122-0.0.313.SE
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:Removing old
image:flash1:c3750-i5-mz.121-19.EA1
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:All software images installed.
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:Requested system reload in progress...
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:Software successfully copied to
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:system(s) 1
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:Done copying software
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:Reloading system(s) 1
```

This example shows that the switch stack detected a new switch that is running a different minor version number than the switch stack. Auto-copy launches but cannot find software in the switch stack to copy to the switch in VM mode to make it compatible with the switch stack. The auto-advise process launches and recommends that you download a tar file from the network to the switch in VM mode:

```
*Mar  1 00:01:11.319:%STACKMGR-6-STACK_LINK_CHANGE:Stack Port 2 Switch 2 has changed to
state UP
*Mar  1 00:01:15.547:%STACKMGR-6-SWITCH_ADDED_VM:Switch 1 has been ADDED to the stack
(VERSION_MISMATCH)
stack_2#
*Mar  1 00:03:15.554:%IMAGEMGR-6-AUTO_COPY_SW_INITIATED:Auto-copy-software process
initiated for switch number(s) 1
*Mar  1 00:03:15.554:%IMAGEMGR-6-AUTO_COPY_SW:
*Mar  1 00:03:15.554:%IMAGEMGR-6-AUTO_COPY_SW:Searching for stack member to act
*Mar  1 00:03:15.554:%IMAGEMGR-6-AUTO_COPY_SW:as software donor...
*Mar  1 00:03:15.554:%IMAGEMGR-6-AUTO_COPY_SW:Software was not copied
```

```
*Mar  1 00:03:15.562:%IMAGEMGR-6-AUTO_ADVISE_SW_INITIATED:Auto-advise-software process
initiated for switch number(s) 1
*Mar  1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:
*Mar  1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:
*Mar  1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:Systems with incompatible software
*Mar  1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:have been added to the stack.  The
*Mar  1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:storage devices on all of the stack
*Mar  1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:members have been scanned, and it has
*Mar  1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:been determined that the stack can be
*Mar  1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:repaired by issuing the following
*Mar  1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:command(s):
*Mar  1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:
*Mar  1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:    archive download-sw /force-reload
/overwrite /dest 1 flash1:c3750-i5-tar.122-18.SE.tar
*Mar  1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:
```

For information about using the **archive download-sw** privileged EXEC command, refer to the "Working with Software Images" section in Appendix B, "Working with the Cisco IOS File System, Configuration Files, and Software Images."

Note Auto-advise and auto-copy identify which images are running by examining the info file and by searching the directory structure on the switch stack. If you download your image by using the **copy tftp:** command instead of by using the **archive download-sw** privileged EXEC command, the correct directory structure is not properly created. For more information about the info file, see the "tar File Format of Images on a Server or Cisco.com" section in Appendix B, "Working with the Cisco IOS File System, Configuration Files, and Software Images."

Additions to the Catalyst 3750 Switch Command Reference

The display for the **show controllers ethernet-controller** command was enhanced to show the XENPAK module serial EEPROM contents. For information about the EEPROM map and the field descriptions for the display, refer to the XENPAK multisource agreement (MSA) at these URLs:

http://www.xenpak.org/MSA/XENPAK_MSA_R2.1.pdf

http://www.xenpak.org/MSA/XENPAK_MSA_R3.0.pdf

To determine which version of the XENPAK documentation to read, check the *XENPAK MSA Version supported* field in the display. Version 2.1 is 15 hexadecimal, and Version 3.0 is 1e hexadecimal.

This is an example of output from the **show controllers ethernet-controller tengigabitethernet1/0/1 phy** command for the 10-Gigabit Ethernet interface:

```
Switch# show controllers ethernet-controller tengigabitethernet1/0/1 phy

TenGigabitEthernet1/0/1 (gpn:472, port-number:1)
----------------------------------------------------------

XENPAK Serial EEPROM Contents:
Non-Volatile Register (NVR) Fields
 XENPAK MSA Version supported         :0x15
 NVR Size in bytes                    :0x100
 Number of bytes used                 :0xD0
 Basic Field Address                  :0xB
 Customer Field Address               :0x77
 Vendor Field Address                 :0xA7
 Extended Vendor Field Address        :0x100
 Reserved                             :0x0
 Transceiver type                     :0x1 =XENPAK
```

```
 Optical connector type               :0x1 =SC
 Bit encoding                         :0x1 =NRZ
 Normal BitRate in multiple of 1M b/s :0x2848
 Protocol Type                        :0x1 =10GgE

Standards Compliance Codes :
 10GbE Code Byte 0                    :0x2 =10GBASE-LR
 10GbE Code Byte 1                    :0x0
 SONET/SDH Code Byte 0                :0x0
 SONET/SDH Code Byte 1                :0x0
 SONET/SDH Code Byte 2                :0x0
 SONET/SDH Code Byte 3                :0x0
 10GFC Code Byte 0                    :0x0
 10GFC Code Byte 1                    :0x0
 10GFC Code Byte 2                    :0x0
 10GFC Code Byte 3                    :0x0
 Transmission range in 10m            :0x3E8
Fibre Type :
 Fibre Type Byte 0                    :0x40 =NDSF only
 Fibre Type Byte 1                    :0x0 =Unspecified

 Centre Optical Wavelength in 0.01nm steps - Channel 0 :0x1 0xFF 0xB8
 Centre Optical Wavelength in 0.01nm steps - Channel 1 :0x0 0x0 0x0
 Centre Optical Wavelength in 0.01nm steps - Channel 2 :0x0 0x0 0x0
 Centre Optical Wavelength in 0.01nm steps - Channel 3 :0x0 0x0 0x0
 Package Identifier OUI  :0x41F420
 Transceiver Vendor OUI  :0x3400871
 Transceiver vendor name :CISCO-OPNEXT,INC
 Part number provided by transceiver vendor       :800-24558-01
 Revision level of part number provided by vendor :01
 Vendor serial number           :ONJ0735003U
 Vendor manufacturing date code :2003082700

 Reserved1 :00 00 00 00 00 00 00
 Basic Field Checksum :0x6C

 Customer Writable Area :
  0x00:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x20:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

 Vendor Specific :
  0x00:41 00 20 F4 88 84 28 94 C0 00 30 14 06 39 00 D9
  0x10:03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x20:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x30:00 00 00 00 11 5E 19 E9 BF 1B AD 98 03 9B DF 87
  0x40:CC F6 45 FF 99 00 00 00 00 00 00 00 00 00 C0 48
  0x50:46 D2 00 00 00 00 00 00 00
```

Related Documentation

These documents provide complete information about the Catalyst 3750, 3560, and 2970 switches and are available at Cisco.com:

- http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/index.htm
- http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3560/index.htm
- http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2970/index.htm

You can order printed copies of documents with a DOC-xxxxxx= number from the Cisco.com sites and from the telephone numbers listed in the "Obtaining Documentation" section on page 66.

These documents provide complete information about the Catalyst 3750 switches:

- *Catalyst 3750 Switch Software Configuration Guide* (order number DOC-7816180=)
- *Catalyst 3750 Switch Command Reference* (order number DOC-7816181=)
- *Catalyst 3750 Switch System Message Guide* (order number DOC-7816184=)
- Cluster Management Suite (CMS) online help (available only from the switch CMS software)
- *Catalyst 3750 Switch Hardware Installation Guide* (order number DOC-7815136=)

These documents provide complete information about the Catalyst 3560 switches:

- *Catalyst 3560 Switch Software Configuration Guide* (order number DOC-7816404=)
- *Catalyst 3560 Switch Command Reference* (order number DOC-7816405=)
- *Catalyst 3560 Switch System Message Guide* (order number DOC-7816406=)
- Cluster Management Suite (CMS) online help (available only from the switch CMS software)
- *Catalyst 3560 Switch Hardware Installation Guide* (order number DOC-7816057=)

These documents provide complete information about the Catalyst 2970 switches:

- *Catalyst 2970 Switch Software Configuration Guide* (order number DOC-7816182=)
- *Catalyst 2970 Switch Command Reference* (order number DOC-7816183=)
- *Catalyst 2970 Switch System Message Guide* (order number DOC-7816185=)
- Cluster Management Suite (CMS) online help (available only from the switch CMS software)
- *Catalyst 2970 Switch Hardware Installation Guide* (order number DOC-7815469=)

For other information about related products, refer to these documents:

- *Cisco Small Form-Factor Pluggable Modules Installation Notes* (not orderable but available on Cisco.com)
- *Cisco RPS 300 Redundant Power System Hardware Installation Guide* (order number DOC-7810372=)
- *Cisco RPS 675 Redundant Power System Hardware Installation Guide* (order number DOC-7815201=)

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.